

2. Enjoin the Defendants from counting any mail-in ballots processed through VR Systems.
3. Order the immediate halt of the implementation of Rule 2.027 and restoration of the removed fields in Form DS-DE 40.
4. Order full transparency and the release of all records regarding the time-stomping and cybersecurity vulnerabilities, including full compliance with public records requests (Exhibits P5-P20), and the release of **originating IP addresses** for all vote-by-mail requests.
5. Enjoin Defendants Wendy Link, Maria Marino, and Robert Weiss from any participation in the November 2024 General Election due to their conspiracy to manipulate the election process.
6. Provide such other relief as this Court deems just and proper.

Respectfully submitted this First day of October, 2024.



Jeff Buongiorno
1901 South Congress Ave, #220
Boynton Beach, FL 33426

EXHIBITS

- **Exhibit P5:** Minutes of the August 9, 2024 Canvassing Board Meeting.

- **Exhibit P6:** Time-stamped Report (Dated September 13, 1984).
- **Exhibit P7:** DS-DE 40 Form with Critical Fields Removed.
- **Exhibit P8:** DS-DE 40 Form Prior to Rule Changes.
- **Exhibit P9:** Documentation Showing Defendant Seconded the Motion to Effectuate Rule 2.027.
- **Exhibit P10:** EL52A Report from the 2022 General Election in Palm Beach County Showing 59 Blank Ballots.
- **Exhibit P11:** EL52 Report from the November 8, 2020 General Election in Palm Beach County Showing 20,313 Blank Ballots.
- **Exhibit P12:** EL52 Report from the November 8, 2020 General Election in Broward County.
- **Exhibit P13:** Evidence of Website Tampering.
- **Exhibit P14:** Email from Defendant Stating She is Not a Canvassing Board Member.
- **Exhibit P15:** VR Systems Terms and Conditions Holding Them Harmless for Data Breaches.
- **Exhibit P16:** Cybersecurity Assessment Report for electionsfl.org Domain.
- **Exhibit P17:** Cybersecurity Assessment Report for VRSYSTEMS.com Domain.
- **Exhibit P18:** VR Systems Memo Dated August 21, 2024 Regarding Primary Election Outage.
- **Exhibit P19:** Buongiorno's Public Records Request for IP Addresses of His Own Vote-by-Mail Request.
- **Exhibit P20:** Letter from Palm Beach Supervisor of Elections' Attorney Accusing a Citizen of a Crime for Challenging Signatures.

UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF FLORIDA

JEFFREY BUONGIORNO,

Plaintiff,

v.

ALEJANDRO MAYORKAS, et al

Case No. 9:24-cv-80920-AMC

ATTESTATION OF AUTHENTICITY OF EXHIBITS

I, Jeff Buongiorno a Pro Se Plaintiff in the above-captioned matter. I hereby certify and attest that the exhibits attached hereto, identified as **Exhibits P5 through P20**, are true, accurate, and complete copies of the original documents, records, and materials from which they were obtained.

These exhibits have been provided in support of the Plaintiff's Motion for Temporary Restraining Order/Injunctive Relief/Other Pleading and are submitted in accordance with the Federal Rules of Civil Procedure and the applicable rules governing the submission of documents in this court.

I declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing is true and correct to the best of my knowledge and belief.

Respectfully submitted and Executed on this First Day of October, 2024

Signed



Jeff Buongiorno

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
CIVIL DIVISION

CASE NO. 9:24-80920-CIV-CANNON

JEFFREY BUONGIORNO,

Plaintiff,

v.

ALEJANDRO MAYORKAS, ET AL

Defendant.

EXHIBIT LIST

By stating specific objections to exhibits, the parties do not alleviate their responsibility to introduce and meet admissibility requirements with respect to any exhibit. The parties may abbreviate objections as needed. The number in the "Exhibit Number" column must indicate the pre-marked identification label (e.g., P-1 or D-1).¹

Exhibit Number	Description	Bates Range / Other Source	Objections and Reasons	Date Identified	Date Admitted
NOTE	P1 to P4 Left Blank Intentionally to accommodate a prior filing.				
P5	Canvassing Board Meeting minutes of August 9 th , 2024	PAGE_0001-PAGE_0002			
P6	Public Records Request #23-92. Time Stamped with 9/13/1984 date.	PAGE_0001-PAGE_0002			
P7	DS-DE 40 Form version 2/2024. Page 0001 1 is Excel	PAGE_0001-PAGE_0002			

¹ The Plaintiffs' exhibits must be marked numerically with the letter "P" as a prefix; the Defendants' exhibits must be marked numerically with the letter "D" as a prefix.

Exhibit Number	Description	Bates Range / Other Source	Objections and Reasons	Date Identified	Date Admitted
	format and Page 0002 is .PDF				
P8	DS-DE 40 used in 2020 Election	PAGE_0001-PAGE_0002			
P9	Canvassing Board meeting minutes from 9/25/2024	PAGE_001-PAGE_0003			
P10	EL52 Report for Nov 8, 2022 Election (59 Blank Ballots cast) PALM BEACH	PAGE-0001			
P11	EL52 Report for NOV 3, 2020 (20,313 Blank Ballots cast) PALM BEACH	PAGE-0001			
P12	EL 52 Report, NOV 8, 2020. Broward County (60,165 Blank Ballots cast)	PAGE-0001			
P13	Witness Affidavit Chris Gleason Attesting to Public Records altering	PAGE_0001-PAGE_0005			
P14	9/26 Email from Supervisor Link stating she is not a member of the canvassing board	PAGE_0001			
P15	VR Terms & Conditions, not liable for protection of data	PAGE_0001			
P16	ElectionsFL.org threat assessment report	PAGE_001-PAGE-PAGE-011			
P17	VRSystems.com threat assessment Report	PAGE_001-PAGE_048			
P18	Vr Systems Memo regarding Outage on 8.20.24	PAGE_001			
P19	Records Request 24-1075	PAGE_001-PAGE_002			
P20	Attorney letter re: contesting Digital Signatures	PAGE_001			



PS - PAGE-0001

2024 PRIMARY ELECTION

August 20, 2024

Friday, August 9, 2024
Vote-by-Mail Ballot Canvassing
10:00 a.m.

(Minutes prepared by Anne Mills)

Present:

Judge Bristow – Canvassing Board Chair (arrived 10:15 a.m.)
Commissioner Weiss – Canvassing Board
Supervisor Link – Canvassing Board

Commissioner Weiss called the meeting to order at 10:12 a.m. and proceeded with roll call. The public notice of the meeting was confirmed and attached to the agenda.

The Canvassing Board reviewed the minutes for the August 2, 2024 Canvassing Board Meeting. Supervisor Link motioned to accept the minutes into the record. Commissioner Weiss seconded the motion, and the motion passed unanimously. Judge Bristow arrived and was added to roll call as present.

Time was provided for members of the public to voice any comments related to items to be discussed as listed on the agenda. Several members of the public presented their comments to the Canvassing Board.

The Canvassing Board commenced with the canvassing of vote-by-mail ballots. Ballots reviewed by the Canvassing Board consisted of ballots referred due to no signatures, signature issues, wrong party, and wrong precinct. During the canvassing of ballots, several objections were made and noted by the Canvassing Board. Two members of the public were removed by Chair Judge Bristow for continued disruptive behavior and disregarding Judge Bristow's numerous requests to conduct themselves with decorum and respectful behavior. Another member of the public was removed for video recording while signatures were being displayed over the public monitors in the canvassing public area.

Ballots protested during public inspection were presented to the Canvassing Board for review. After reviewing the protested ballots, Supervisor Link provided a summary of the process staff must undertake to prep the ballot and research documentation necessary for the Canvassing Board prior to the meeting. Ballots/signatures were presented for review, with three separate submissions from one person, and another set from a separate person, all of which had signatures that were clearly matching the signature on file. The Canvassing Board determined that frivolous challenges were being made, thereby abusing the public inspection process. A review of a third person's submission was made, and while all signatures were accepted by the Canvassing Board, it was not unanimously agreed that the third set was frivolous. The staff time involved was substantial as well as time of the Canvassing Board to review the frivolous challenges. The Canvassing Board discussed a mechanism to discourage abuse of the process. The Canvassing Board agreed to send a letter of notice to offenders by legal counsel on behalf of the Canvassing Board that they will be referring frivolous challenges to the Office of Election Crimes and Security.

15 - PAGE-0002

The Canvassing Board discussed the newly adopted Rule 1S-2.027 to include DS-DE 420 Standards for Determining Voter Intent. The Voter Intent Addendum was reviewed and agreed upon for the 2024 Primary Election. The Canvassing Board will utilize the DS-DE 420 and the Voter Intent Addendum for guidance, with particular attention to consistency on the ballot markings. Judge Bristow motioned that true under-voted ballots with no markings (stray or otherwise) throughout the ballot will be presented to the Canvassing Board to confirm that it is a truly blank ballot before SOE Staff processes it. Ballots with any markings will be presented to the Canvassing Board for review. Supervisor Link seconded the motion, and the motion passed unanimously.

The Canvassing Board was presented with duplicated ballots for voter intent determination. The Canvassing Board discussed ballots with clear over votes. Ballots with clear over votes with no voter intent issues will be tabulated without duplication. Ballots with any mark other than clear over votes will be presented to the Canvassing Board for voter intent determination.

A listing of meeting breaks of the Canvassing Board for the day is provided below:

11:29 a.m. – 10:35 a.m. 11:59 p.m. – 12:58 p.m.

Judge Bristow adjourned the meeting at 4:11 p.m.

P6 PAGE-0001

Palm Beach County - SOE Public Records

Documents have been released for record request #23-92 along with the following message:

Per your request attached please find the EL45A and the EL52. I will be forwarding you an invoice via PayPal for the EL30A fulfillment.

The estimate is only for the 2022 General Election EL30A.

- [EL45A - General Election 2022.txt](#)
- [EL52 - General Election_Redacted.pdf](#)

[View Request 23-92](#)

<https://palm-beach-county-soe-fl.nextrequest.com/requests/23-92>

Document links are valid for one month. After June 1, you will need to sign in to view the document(s).

P6

PAGE - 0002

Fw: PBC - Altering, Forging Official Election Documents

Jeff Buongiorno <Jeff@etektraining.com>

Sat 8/31/2024 12:15 PM

To:Jeff Buongiorno <Jeff@etektraining.com>

This EL45A Report was sent this morning from the PBC SOE Office

20 20 30 40 50 60 70 80 90 100 110 120 130		OFFICIAL GENERAL ELECTION November 8, 2022 Palm Beach County		OFFICIAL RESULTS	
SUMMARY REPORT-GROUP DETAIL		Report EL45A Page 001			
Run Date 09/11/2024 04:23 AM					
TOTAL VOTES	%	RD	VRM	RV	
REGISTRATION CURRENT (as of 7/29/2024)		395	100.00		
REGISTERED VOTERS - TOTAL		1001,678			
BALLOOT CAST - TOTAL		945,950			
BALLOOT CAST - BALLOT		945,950			
VOTER TURNOUT - TOTAL		94.26			
VOTER TURNOUT - BALLOT		.94			
UNITED STATES SENATE					
(VOTE FOR 1)					
Marco Rubio (RWP)		267,718	48.32	319,763	76,633
Val Demings (DEM)		266,618	48.11	71,830	184,241
Deb Haaland (DLP)		1,800	.33	703	725
Steven B. Grant (RPA)		2,248	.43	807	932
Tom T. Rogers (RPA)		1,010	.19	706	620
WHITE-IB		348	.06	94	80
Over Votes		117		63	0
Under Votes		2,501		1,625	463

After receiving this report we requested the EL52 and EL30A Report for the same election. Something interesting happened after the request. The EL45A File in the PBC SOE Portal Changed.

This is what the NEW and improved report looked like:

New Run Date, However the verification hash at the top of the page was gone.

Why?

Run Date 09/11/2024 04:23 AM	Where is the hash?
	How did the date change?

When we look at the EL52 we can see some interesting data.
Fractional votes...

P7

Entered on FLSD Docke
PAGE - 0001

File Home Insert Page Layout Formulas Data Review View Automate Help Acrobat

Clipboard Paste Font Alignment Number Styles Cells Editing Sensitivity Add-ins Analyze Data Create PDF and Share link Share via Outlook Adobe Acrobat

E10

A B C D E F G H I J K L M N O P Q R S T U V W X



General Election Report On Overvotes And Undervotes
(Section 101.595(1), Fla. Stat.) (Due to the Division of Elections no later than December 15th of the General Election year)

Section I
Information/Summary
The data in **Section I** pertains to this election.
General Election Year:
County Name:
Registered Voters:

Section II
Ballot Design
The data in **Section II** is for ballot design only. Please put an "X" in all boxes that apply. Refer to the Instructions worksheet, if needed.

PJ **PAGE - 0002**

General Election Report On Overvotes And Undervotes (Section 101.595(1), Fla. Stat.) (Due to the Division of Elections no later than December 15th of the General Election year)					
Section I Information/Summary The data in Section I pertains to this election. General Election Year: 1 <u>2024</u> County Name: 2 <u></u> Registered Voters: 3 <u></u>					
Section II Ballot Design The data in Section II is for ballot design only. Please put an "X" in all boxes that apply. Refer to the Instructions worksheet, if needed.					
Ballot Language 1 <input type="checkbox"/> English only 2 <input type="checkbox"/> Multi-Language - All languages on one ballot 3 <input type="checkbox"/> Multi-Language - Each language on a separate ballot	Rule Deviations 12 <input type="checkbox"/> There were more candidates than would fit in one column or screen 13 <input type="checkbox"/> The candidate's name was longer than would allow the party abbreviation to fit to the right of the candidate's name Instructions 14 <input type="checkbox"/> A candidate's name was too long to fit on one line in the minimum font size 15 <input type="checkbox"/> The party abbreviation could not be printed in the minimum font size without going onto a second line Contest Title 16 <input type="checkbox"/> Printing the (Vote for X) designations in the minimum font size would have required require an additional ballot card 17 <input type="checkbox"/> The voting system does not permit the suppression of party abbreviations when a universal primary contest exists 18 <input type="checkbox"/> An other extraordinary circumstances which could not reasonably be accommodated except by deviation from the requirements of the rule. <u>Describe in the Comments below.</u>				
Comments: <hr/>					
Section III Possible Factors Affecting Undervotes and Overvotes Please put an "X" in all boxes that apply. Refer to the Instructions worksheet, if needed.					
Voting System 19 <input type="checkbox"/> Voter Instruction Issue 20 <input type="checkbox"/> Voting Equipment Issue 21 <input checked="" type="checkbox"/> New Voting System	Ballot Length 22 <input type="checkbox"/> Single Card 23 <input type="checkbox"/> Multiple Card If multiple Cards, how many? 24 <u></u>				
Other 25 <input type="checkbox"/> Natural Disaster 26 <input type="checkbox"/> Other: Please Explain	Comments: <hr/>				
Section IV Report Results for: President and Vice President The data in Section IV is for this race only. Please fill in all numbered boxes. Refer to the Instructions worksheet, if needed. NOTE: Only totals from the Election Day Database should be used. Do Not use totals from machine or manual recount.					
Are Provisional ballots included in Group Totals (EV, ED, VBM) ↓ Check if Yes		Votes Cast for the office above: Total # of Votes cast including all write-ins ↓ Undervotes Do Not Include in "A" ↓ Overvotes Do Not Include in "A" ↓			
Early Voting 27 <input type="checkbox"/> Election Day 33 <input type="checkbox"/> Vote-by-Mail 39 <input type="checkbox"/> Provisionals Accepted 45 <input type="checkbox"/>		A 28 <input type="checkbox"/> 34 <input type="checkbox"/> 40 <input type="checkbox"/> 45 <input type="checkbox"/>	B 29 <input type="checkbox"/> 35 <input type="checkbox"/> 41 <input type="checkbox"/> 46 <input type="checkbox"/>	C 30 <input type="checkbox"/> 36 <input type="checkbox"/> 42 <input type="checkbox"/> 47 <input type="checkbox"/>	← G <input type="checkbox"/> D <input type="checkbox"/> E <input type="checkbox"/> F <input type="checkbox"/>
Column total A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/>		Valid Write-In ↓ E <input type="checkbox"/> Invalid Write-In ↓ F <input type="checkbox"/>			
Grand Total = Sum of cells A + B + C Grand Total = <u></u>					
Section V County Comments For President and Vice President Race					
DS-DE-40 rev. 02/2024					

P8

PAGE - 0001

File Home Insert Page Layout Formulas Data Review View Automate Help Acrobat
 PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing

AC77

A B C D E F G H I J K L M N O P Q R S T U V W X

1 FLORIDA ELECTIONS

2

3

4

5 SECTION I:

6 The data in Section I pertains to this election.

7 General Election Year 1 2020

8 County Name 2 Orange

9 Registered Voters 3 888,460

10 Duplicated Ballots 4 5,527

11 Blank Ballots 5 22,719

12

13 SECTION II:

14 Ballot Design

15 The data in Section II is for ballot design only. Please put an "X" in all boxes that apply. Refer to the Instructions worksheet, if needed.

16

17

18 Ballot Language

19 11 English only

19 Rule Deviations

19 There are more candidates than will fit in one column or screen



GENERAL ELECTION REPORT ON OVERVOTES AND UNDERVOTES
(Section 101.595(1), Fla. Stat.) (Due by December 15th of General Election year)

SECTION I:*The data in Section I pertains to this election.*

General Election Year	1	2020
County Name	2	Orange
Registered Voters	3	866,460
Duplicated Ballots	4	5,527
Blank Ballots	5	22,719

Provisional Ballots Accepted	6	184
Provisional Ballots Rejected	7	329
Vote-by-Mail Ballots Requested	8	341,363
Vote-by-Mail Ballots Accepted	9	277,476
Vote-by-Mail Ballots Rejected	10	776

SECTION II:**Ballot Design***The data in Section II is for ballot design only. Please put an "X" in all boxes that apply. Refer to the Instructions worksheet, if needed.*

Ballot Language
 11 English only
 12 Multi-Language - All languages on one ballot
 13 Multi-Language - Each language on a separate ballot

Instructions
 14 Ballot Instructions - Across page - Centered
 15 Ballot Instructions - Across page - Flush Left
 16 Ballot Instructions - Leftmost Column

Contest Title
 17 Contest Title - No Background
 18 Contest Title - Shaded Background

Rule Deviations
 19 There are more candidates than will fit in one column or screen
 20 The candidate's name is longer than will allow the party abbreviation to fit to the right of the candidate's name
 21 A candidate's name is too long to fit on one line in the minimum font size
 22 The party Abbreviation cannot be printed in the minimum font size without going onto a second line
 23 Printing the (Vote for X) designations in the minimum font size will require an additional ballot card
 24 The voting system will not permit the suppression of party abbreviations on ballots when a universal primary contest exists
 25 Any other extraordinary circumstances which cannot reasonably be accommodated except by deviation from the requirements of the rule. Describe in the Comments below:

Comments:**Section III:****Possible Factors Affecting Undervotes and Overvotes***Please put an "X" in all boxes that apply. Refer to the Instructions worksheet, if needed.*

Voter Interest
 26 Federal Contest - High
 27 Federal Contest - Low
 28 State Contest - High
 29 State Contest - Low
 30 Local Contest - High
 31 Local Contest - Low
 32 Amendment - High
 33 Amendment - Low
 34 Referendum - High
 35 Referendum - Low

Media Coverage
 36 National - High Level
 37 National - Low Level
 38 National - Positive Coverage
 39 National - Negative Coverage
 40 Local - High Level
 41 Local - Low Level
 42 Local - Positive Coverage
 43 Local - Negative Coverage

44	Voter	51	Other
	National Literature/Advertisement - High		Natural Disaster
45	Voter Literature/Advertisement - Low	52	Other: Please Explain
46	Election Perception - Positive		
47	Election Perception - Negative		
48	Voting System		
49	Voter Instruction Issue		
50	Voting Equipment Issue		
51	New Voting System		

Comments:**SECTION IV:****Report Results for: President and Vice President***The data in Section IV is for this race only. Please fill in all numbered boxes. Refer to the Instructions worksheet, if needed.**NOTE: Only totals from the Election Day Database should be used. Do Not use totals from machine or manual recount.*

	Check if Yes	Votes Cast for the office above:			Valid Write-In	Invalid Write-In
		Total # of Votes cast	Undervotes	Overvotes		
		including all write-ins	Do Not include in "A"	Do Not include in "A"		
Early Voting	53	<input type="checkbox"/>	54 262,240	55 482	56 222	57 538
Election Day	59	<input type="checkbox"/>	60 109,258	61 405	62 121	63 488
Vote-by-Mail	65	<input type="checkbox"/>	66 277,476	67 983	68 1,735	69 728
Provisionals Accepted	71	<input type="checkbox"/>	72 183	73 -	74 1	75 -
		A	B	C	E	F
		Column total	649,157	1,870	2,079	
					D 184	E 1,754
					F 107	

Grand Total = Sum of cells A + B + C

Grand Total = 649,157

Matches Provisional Ballots Accepted

Section V: County Comments For President and Vice President Race



2024 GENERAL ELECTION

November 5, 2024

P9

PAGE-6001

Wednesday, September 25, 2024
Pre-Election Canvassing Board Meeting
2:00 p.m.

(Minutes prepared by Anne Mills)

Present:

Judge Bristow – Canvassing Board Chair
Vice Mayor Marino, Canvassing Board
Commissioner Weiss – Canvassing Board
Judge Tew – Canvassing Board Alternate
Judge Silver – Canvassing Board Alternate
Director Jacobowitz, Canvassing Board Alternate
Supervisor Link – Advisor

Judge Bristow called the meeting to order at 2:10 p.m. and proceeded with roll call. The public notice of the meeting was confirmed and attached to the agenda. Commissioner Weiss made a motion to approve the public notice into the record and Judge Bristow seconded the motion. The motion passed unanimously, and the notice was entered into the record.

Time was provided for members of the public to voice any comment for items to be discussed as listed on the agenda or any canvassing related items for the 2024 General Election. Comment cards were provided and located on the public access table along with the agenda. After all comments submitted were heard by the Canvassing Board, Commissioner Weiss made a motion to defer any responses to the comments presented until all items on the agenda have been addressed, if time permits. Vice Mayor Marino seconded the motion, and the motion passed unanimously.

The Canvassing Board reviewed the proposed canvassing schedule for the 2024 General Election. After discussion and adjustments, Judge Bristow made a motion to accept the canvassing schedule and Vice Mayor Marino seconded the motion. The motion was passed unanimously.

Judge Bristow provided an overview of the rules of the canvassing room/area and standards of conduct as outlined on the agenda:

- Phones are to be silent and prohibited from being used in the canvassing area.
- Photography and video recordings of any ballots and signatures are not permitted at any time during the election process to include the canvassing area or during duplication.
- Standards of Conduct
 - o All parties are to act with decorum and respect.
 - o The public may observe the canvassing process; however, the Canvassing Board is not required to take questions or engage in any discussions with the public.
 - o There will be no discussion during the canvassing process.

P9

PAGE - 0002

- Any person causing a disruption or breaking the rules of the proceedings will be given one warning. If the disruption continues, they will be asked to leave and will be barred for the duration of the election cycle (through the General Election).

Vice Mayor Marino made a motion to accept the rules of the canvassing room/area and standards of conduct as outlined above, and Commissioner Weiss seconded the motion. The motion passed unanimously, and the rules and standards were adopted.

Judge Bristow provided an overview of the objection procedures for signature verification, duplication, and public inspection.

- Signature Verification – Objections will be heard and noted. No other discussion will be entertained.
- Duplication – Objections will be noted in the minutes to include duplication numbers as required by statute.
- Public Inspection – A blanket objection to all applicable certificates/signatures in canvassing will be noted once, as these objections have already been noted during the public inspection process.

Objections were made by members of the public regarding the objection procedures outlined for consideration. Vice Mayor Marino made a motion to accept the objection procedures as outlined, Commissioner Weiss seconded the motion. The motion passed unanimously.

The Canvassing Board discussed the canvassing guidelines as outlined in the agenda.

- Ballot Envelope Signature Location – A signature located anywhere on the voter certificate side of the ballot will be considered by The SOE staff and/or Canvassing Board during the signature verification process.

Objections were made by the public regarding signature location on the envelope certificate/staff processing. Commissioner Weiss made a motion to accept the signature location guideline as outlined, Vice Mayor Marino seconded the motion. The motion passed unanimously.

- True under-voted ballots with no markings (stray or otherwise) throughout the ballot will be processed by SOE Staff. Ballots with any markings will be presented to the Canvassing Board for review.
- Ballots with clear overvotes will be processed by SOE Staff. Ballots with any voter intent issues will be presented to the Canvassing Board for review.

Objections were made by members of the public regarding the handling of over and under voted ballots.

Commissioner Weiss made a motion to have SOE staff review and process true overvoted or under voted ballots as outlined and Vice Mayor Marino seconded the motion. The motion passed unanimously.

- Duplication review per F.S. 101.5614(4)(a) states objections during duplication may be made by those qualified as outlined in statute. Palm Beach County has provided the public with the opportunity to make objections during duplication. Judge Bristow recommended that the policy of allowing members of the public to make objections during duplication continue through this election if there is no abuse and will reserve the right to revisit the policy if needed.

Commissioner Weiss motioned to continue with the duplication process as recommended and Vice Mayor Marino seconded the motion. The motion passed unanimously.

- The Canvassing Board reviewed the Voter Intent Addendum to supplement voter intent standards as set in DS DE 420.

P9

PA 66-0003

During the review process of the voter intent addendum, objections were made by the public. Vice Mayor Marino motioned to accept the Voter Intent Addendum with determinations made by the Canvassing Board to be used in conjunction with the DS DE 420 for the 2024 General Election, Judge Bristow seconded the motion, and the motion passed.

Supervisor Link provided an overview of the processing of ballots protested during public inspection.

- Protested ballots will be segregated for second review. If SOE staff agree with the protest, a signature cure affidavit will be sent to the voter, the ballot marked provisionally rejected and presented to the Canvassing Board for review. If the staff does not agree with the protest, the ballot will be submitted to the Canvassing Board for review. All protested ballots will be notated with a blanket objection.

Objections were made by members of the public regarding the handling of protested ballots during public inspection.

- Staff to open and process ballot envelopes once they have been accepted by SOE staff without any objections or have been accepted by the Canvassing Board.

Objections were made by members of the public regarding the staff processing of accepted ballot envelopes.

Judge Bristow provided Supervisor Link the opportunity to respond to comments made during the comment portion of the Canvassing Board Meeting. A member of the public was removed by Chair Judge Bristow for continued disruptive behavior and disregarding Judge Bristow's numerous requests to conduct themselves with decorum and respectful behavior.

Judge Bristow referred to the agenda to discuss the guideline for handling ballots with mismatched signatures.

- Household signature mismatch – any signature mismatch for which a member of the same household signs the wrong ballot envelope will be counted if both parties have vote-by-mail requests on file and the signature is verified to match the signature on record.
- Staff to accept mismatch ballots meeting the criteria above, all others will be presented to the Canvassing Board for review.

Objections were made by members of the public regarding the handling of mismatched ballots. Vice Mayor Marino motioned to accept ballots that meet the criteria as outlined for mismatched signatures, Judge Bristow seconded the motion. The motion passed unanimously.

Judge Bristow adjourned the meeting at 3:42 p.m.

P10

PAGE - 0001

NUMBERED KEY CANVASS
OFFICIAL RESULTS

Run Date: 05/01/23 09:58 AM

REPORT-EL52

Official General Election

November 8, 2022

Palm Beach County, Florida

PAGE 0001

	TOTAL	PERCENT	TOTAL	PERCENT
01 = REGISTERED VOTERS - TOTAL			1003,675	03 = BALLOTS
CAST - BLANK	59			
02 = BALLOTS CAST - TOTAL			545,550	04 = VOTER
TURNOUT - TOTAL		54.36		
	01	02	03	04
1401 1401	1869	1368	. . 0	73.19
1501 1501	1924	. 885	. . 0	46.00
1502 1502	1986	1000	. . 0	50.35
1503 1503	1737	. 830	. . 0	47.78
1505 1505	737	. 375	. . 0	50.88
1506 1506	2174	1246	. . 0	57.31
1507 1507	2092	1062	. . 0	50.76
1508 1508	497	. 142	. . 0	28.57
1509 1509	1104	. 416	. . 0	37.68
1510 1510	506	. 213	. . 0	42.09
1511 1511	244	. 108	. . 0	44.26
1512 1512	894	. 328	. . 0	36.69
1513 1513	284	. 134	. . 0	47.18
1514 1514	1156	. 389	. . 0	33.65
1515 1515	1086	. 540	. . 0	49.72
1516 1516	780	. 245	. . 0	31.41
1517 1517	1390	. 783	. . 0	56.33
1518 1518	1310	. 405	. . 0	30.92
1519 1519	1756	1189	. . 0	67.71
1520 1520	1384	. 911	. . 1	65.82
1521 1521	1660	. 948	. . 0	57.11
1523 1523	281	. 151	. . 0	53.74
1524 1524	1526	. 539	. . 0	35.32
1525 1525	1997	1130	. . 0	56.58
1526 1526	1299	. 762	. . 0	58.66
1527 1527	966	. 582	. . 0	60.25
1528 1528	1213	. 796	. . 0	65.62
1529 1529	2085	1513	. . 0	72.57
1530 1530	281	. 145	. . 0	51.60
1531 1531	475	. 189	. . 0	39.79
1532 1532	1649	1033	. . 0	62.64
1537 1537	2382	. 825	. . 1	34.63
1538 1538	1515	. 662	. . 0	43.70
1539 1539	2356	. 781	. . 0	33.15

P11

PAGE-0002

[REDACTED]

NUMBERED KEY CANVASS

OFFICIAL RESULTS

RUN DATE: 05/03/23 12:13 PM

REPORT-EL52

PAGE 0001

Official General Election

Palm Beach County Florida

November 3, 2020

	TOTAL	PERCENT	TOTAL	PERCENT
01 = REGISTERED VOTERS - TOTAL			1019,884	03 = BALLOTS
CAST - BLANK	20,313			
02 = BALLOTS CAST - TOTAL			778,201	04 = VOTER
TURNOUT - TOTAL		76.30		
	01	02	03	04
1002	0			
1004	11			
1006	0			
1008	0	.	0	.
1010	0	.	0	.
1012	0	.	0	.
1014	1			
1016	0	.	0	.
1018	1823	1516	.	17 83.16
1019	807	674	.	11 83.52
1020	0	.	0	.
1022	2817	2331	.	33 82.75
1024	20	.		
1026	1343	1125	.	17 83.77
1028	2190	1829	.	35 83.52
1030	88	71	.	0 80.68
1032	1256	1080	.	14 85.99
1034	1280	1174	.	12 91.72
1036	0	.	0	.
1038	2953	2495	.	35 84.49
1040	1113	943	.	14 84.73
1042	0	.	0	.
1044	746	534	.	16 71.58
1046	609	377	.	9 61.90
1048	1285	1050	.	27 81.71
1050	1677	1417	.	27 84.50
1052	3286	2521	.	40 76.72
1054	2555	2147	.	35 84.03
1056	1788	1366	.	28 76.40
1058	2563	1991	.	41 77.68
1060	274	197	.	3 71.90
1062	2436	2070	.	35 84.98
1064	275	235	.	0 85.45
1066	0	.	0	.

The Wayback Machine - <https://web.archive.org/web/20230131060422/https://www.browardvotes.gov/Portals/B...>

PI 2
 PAGE - 0001
 0E0&12a007c067F0(s0p16.66h3b6T0&a00L
 SUMMARY REPT-GROUP DETAIL
 REPORT-EL45A PAGE 001

2022 GENERAL ELECTION

NOVEMBER 8, 2022
 BROWARD COUNTY, FLORIDA

RUN DATE: 11/18/22 05:00 PM

EV	PV	TOTAL VOTES	%	ED	AV
PRECINCTS COUNTED (OF 355)		355	100.00		
REGISTERED VOTERS - TOTAL		1252,776			
BALLOTS CAST - TOTAL		600,976		186,804	225,722
188,379	71				
BALLOTS CAST - BLANK		60,165	10.01	22,321	19,582
18,251	11				
VOTER TURNOUT - TOTAL			47.97		
VOTER TURNOUT - BLANK			4.80		

United States Senator

(VOTE FOR) 1

(WITH 355 OF 355 PRECINCTS COUNTED)

Marco Rubio (REP)	238,962	39.95	92,986	61,134
84,806	36			
Val Demings (DEM)	353,575	59.11	90,554	161,290
101,698	33			
Dennis Misigoy (LPF)	2,081	.35	830	730
521	0			
Steven B. Grant (NPA)	2,083	.35	747	912
423	1			
Tuan TQ Nguyen (NPA)	1,223	.20	445	548
230	0			
WRITE-IN (NPA)	243	.04	109	79
55	0			
Over Votes	224		74	108
42	0			
Under Votes	2,585		1,059	921
604	1			

Representative in Congress District 20

(VOTE FOR) 1

(WITH 102 OF 102 PRECINCTS COUNTED)

Drew Montez Clark (REP)	34,200	25.12	13,359	9,228
11,603	10			
Sheila Cherfilus-McCormick (DEM)	101,958	74.88	25,907	45,544
30,496	11			
Over Votes	17		5	9
3	0			
Under Votes	5,622		1,166	3,532
923	1			

Representative in Congress District 23

(VOTE FOR) 1

(WITH 103 OF 103 PRECINCTS COUNTED)

Joe Budd (REP)	88,137	45.07	35,810	22,132
30,184	11			
Jared Moskowitz (DEM)	104,053	53.21	26,213	48,795
29,035	10			
Mark Napier (NPA)	1,020	.52	394	409
217	0			
Christine Scott (NPA)	2,327	1.19	948	816

PAGE - 0001

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
CIVIL**

Jeffrey Buongiorno, Plaintiff

v.

Alejandro Mayorkas, et al, Defendant

Case No.: 9:24-cv-80290-AMC

**AFFIDAVIT OF CHRISTOPHER GLEASON
REGARDING CHAIN OF CUSTODY FOR STATEWIDE VOTE BY MAIL
EARLY VOTING LIST**

STATE OF FLORIDA

COUNTY OF PINELLAS

BEFORE ME, the undersigned authority, personally appeared Christopher Gleason, who, being duly sworn, deposes and says as follows:

1. Affiant's Identity:

My name is Christopher Gleason. I am over the age of 18, competent to make this affidavit, and have personal knowledge of the facts stated herein.

2. Purpose of Affidavit:

PARK-0002

P13

This affidavit is made to establish the chain of custody for the Statewide Vote By Mail Early Voting List (the "Voting List") that I obtained directly from the Florida Division of Elections at the following url:

<https://countyballotfiles.floridados.gov/VoteByMailEarlyVotingReports/Reports>

3. Acquisition of Voting List:

On or about and between the dates of 07/14/2024 – 09/29/2024, I personally accessed the Florida Division of Elections secure online system for authorized individuals as clearly stated in FL Stat 101.62 and FAC 1S-2.043. I used the following secure URL

<https://countyballotfiles.floridados.gov/VoteByMailEarlyVotingReports/Reports> provided to me by the Division of Elections to download the daily updates of the Statewide Vote By Mail Early Voting List.

4. Secure Download Process:

The Florida Division of Elections provided me access to the Voting List via the following secure link

<https://countyballotfiles.floridados.gov/VoteByMailEarlyVotingReports/Reports> , which required my unique login credentials provided by the Division. These credentials were assigned specifically for my use as a registered recipient of the

P13 PAGE-0003

Voting List after directly registering with the State at the following url:

<https://countyballotfiles.floridados.gov/Account/Register>

5. Receipt of Voting List:

Upon logging into the secure platform between the dates of 07/14/2024 to 09/29/2024, I downloaded the Voting List, which was provided in .txt and/or .zip format. I saved the downloaded files directly to my computer under secure conditions, ensuring that the data was not altered.

6. Handling and Storage:

After downloading the Voting List, I took immediate steps to preserve the integrity of the data. The files were securely stored on my computer, which is protected by encryption and password protection. No unauthorized individuals had access to the Voting List from the time I downloaded it until it was submitted in connection with this case.

7. Integrity of the Data:

I affirm that the Voting List downloaded from the Florida Division of Elections has not been altered, modified, or tampered with in any way. The files I obtained are in the same condition as when I downloaded them directly from the Division's secure platform.

P13

PAGE - 0004

8. Submission of Voting List:

I am submitting the Voting List as evidence in this case. The data submitted is a true and accurate copy of what I obtained from the Florida Division of Elections, and it is presented in its original, unaltered form.

9. Affirmation of Chain of Custody:

I attest that I was the sole individual who downloaded, handled, and maintained the Voting List from the time of its acquisition until its submission in this case. The chain of custody has remained intact, and there have been no unauthorized accesses or alterations to the Voting List.

10. Illegally Requested Vote By Mail Ballots/ Altered Vote By Mail Election Records

I attest that on 09/03/2024 I reviewed the Pinellas County and Miami Dade Vote By Mail Ballot Reports.

The Pinellas County Report showed that 219,675 Vote By Mail Ballots were requested on Sunday 06/23/2024.

The Miami-Dade County Report showed that 179,357 Vote By Mail Ballots were requested on 06/26/2024.

PB3 PAGE -5

I attest that on 09/29/2024 I reviewed the Pinellas County Report, it showed that there were now 20 Requests for Vote By Mail Ballots requested on 06/23/2024 and that now 198,166 requests for Vote By Mail Ballots were made on 09/09/2024.

I attest that on 09/29/2024 I reviewed the Miami-Dade County report, it now showed that on 06/26/2024 that there were 0 requests made for Vote By Mail Ballots on 06/26/2024 and that there were 249,924 requests for Vote By Mail Ballots made on 09/13/2024.

11. Public Records Requests Made To Miami Dade and Pinellas County Supervisor of Elections Offices.

Public Records Requests were made to both the Pinellas County and Miami-Dade County Supervisor of Elections Offices for the Public Records/ Election Records of the IP Addresses of the voters who made the Vote By Mail Ballot Requests on 06/23/2024 and 06/26/2024. In both cases the custodian of records stated that there were no "Responsive Records" related to these Vote By Mail Requests.

PCB

PAGE - 0006

FURTHER AFFIDAVIT OF PLAINTIFF

Dated this 29 day of September 2024



Christopher Gleason

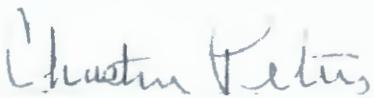
Plaintiff

NOTARY ACKNOWLEDGMENT

STATE OF FLORIDA

COUNTY OF PINELANDS

SWORN TO and subscribed before me this 29th day of Sept 2024 by
Christopher Gleason, who is personally known to me or who has produced a
Drivers License as identification



Notary Public

State of Florida

My Commission Expires [insert date].

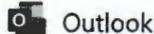
[Seal]



CHRISTINE PETERS
Commission # HH 496653
Expires February 26, 2028

P14

PAGE 0001

**RE: Forceful Removal for Asking Questions****From** Wendy Link <wendy@votepalmbeach.gov>**Date** Thu 9/26/2024 6:36 PM**To** TODD BUFFINGTON <todd.buffington@flgov.com>**Cc** Jeff Buongiorno <jeff@elektraining.com>, K. Meckert <kmeckert@protonmail.com>, Carl Cascio <carl@bellsouth.net>, Kristo Mondo <thermondos@protonmail.com>, Kevin Neal <neal.kj@gmail.com>, Michael Kelly <mkelly@collins.com>, Jennifer K. Kelly <jennifekelly@collins.com>, Patty Frei <patty.frei@flgov.com>, Barbara Sarnelle <bsarnelle@flgov.com>, Mark Foxworth <mark.foxworth@flgov.com>, Paul D. Dickey <pdickey@flgov.org>, Christopher G. Gandy <cgandy@flgov.com>, Tom Spina <tom.spina@flgov.com>

Dear Mr. Buffington,

Your allegations and accusations are **not accurate**. A few notable and important clarifications:

- I did not remove nor request the removal of anyone at the Canvassing Board meeting. The Chair, Judge Bristow, after several warnings to the individual, requested that she be removed from the meeting. I am **NOT a member of this Canvassing Board**, and therefore could not have someone removed from their meeting. I am there in an advisory capacity only, to answer questions that the Canvassing Board may have about our procedures. This is a prime example of the **misinformation** that is being spread by you and others.
- Judge Bristow warned the individual and all others in the audience on multiple occasions that they were not to disrupt the business of the Canvassing Board. When the individual continued to disrupt the meeting (conveniently missing from the video clip you referenced), Judge Bristow asked that she be removed. When she refused to peacefully leave, the Sheriff Deputies escorted her out. (This dramatic and theatrical exit appeared to have been fully orchestrated by those in attendance.)
- All individuals in attendance were given the opportunity to speak at the start of the Canvassing Board meeting. Chair Bristow even gave extra time for anyone who wanted to submit a comment card. No one was denied the ability to speak at that appropriate time.
- The Canvassing Board members asked if I would be willing to answer questions at the end of the meeting that had been asked by those present in the audience. I agreed that I would be happy to answer every question at whatever time the Canvassing Board deemed appropriate. I was in the process of answering those questions when Ms. Frei, after continuing to interrupt, was asked by Judge Bristow to leave. No one was removed for asking too many questions. I was answering every question, including the question about the use of automatic signature verification that you reference (which we do not use).

I have forwarded your message to our public records department, and they will respond to you regarding your public records requests if they have not already.

Wendy Sartory Link*Supervisor of Elections*

Master Florida Certified Elections Professional
Certified Election Registration Administrator

P: (561) 656-6200
D: (561) 656-6261
F: (561) 656-6287

WE'VE MOVED! Voting in Palm Beach County just got **BETTER**.



215
PACF - GO1

17. **Assignment; Binding Effect.** Neither party hereto may assign its right or obligations under this Agreement without the prior written consent of the other party except that VRS may assign this Agreement to any entity which acquires all or substantially all of its business by merger, sale of assets, or otherwise. Without the prior written approval of VRS, neither the Agreement or the License herein granted may be sub-licensed, transferred, given, assigned to, or leased or used by, any third party including but not limited to Customer's consultants or other contractors or governmental entities. Any such transfer is of special concern as it involves any present or potential competitor of VRS, or anyone who might develop systems similar to the System, or who might use VRS' proprietary information in any manner whatsoever. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the parties' permitted assigns and successors.
18. **Installation Responsibility.** Customer shall be solely responsible for site preparation, including unpacking, uncrating, and installing the hardware and making the hardware ready for operational use. The installation of all necessary cable, power connections, utility, network and communications services shall be performed by Customer.
19. **No Liability for Privacy of Information.** Due to the public nature of the Internet, all information should be considered publicly accessible, and important or private information should be treated carefully by Customer. VRS is not liable for protection or privacy of information transferred through the Internet or any other network provider that customers may utilize.
20. **Progress Reports/Meetings.** VRS and Customer shall, within thirty (30) days of this Agreement signing, jointly develop a Project Management Plan, "Exhibit F", which shall be attached to this Agreement as "Exhibit F", detailing tasks to be performed, responsibility for the accomplishment of each task, and a deadline for each task. Customer and VRS will conduct meetings to review progress on a regular basis, with the schedule to be jointly determined.
21. **Maintenance and Support.**
(a) **Coverage.** During the Initial Term of this Agreement, subject to renewal or termination as otherwise provided, VRS agrees to:

VoterFocus*

Palm Beach County Contract 2 & 19

Page 7

P16

PART - 0001

1. **Affiliate Information Analysis**

- **Domain**: Website-related affiliates such as companies, domains, and emails.
- **Expert**: Cybersecurity and network intelligence expert.
- **Keywords**: Affiliate domains, company names, email addresses, internet names.
- **Assumptions**: The data includes a network of related entities, such as companies, domains, and emails associated with the target website.
- **Approach**:
 - Identify common affiliates associated with domains, emails, and IP addresses.
 - Examine any patterns or potential risks associated with the affiliates.

2. **Networking and Hosting Analysis**

- **Domain**: Network architecture and hosting.
- **Expert**: Network infrastructure and hosting provider analyst.
- **Keywords**: IP addresses, netblocks, BGP, hosting providers.
- **Assumptions**: The IP addresses and netblocks can provide insights into the infrastructure of the website.
- **Approach**:
 - Assess the distribution of IP addresses and hosting providers.
 - Look for any patterns that might indicate shared infrastructure across affiliates.
 - Investigate any BGP memberships to see if the website has any relationships with major internet providers.

3. **Security and Malicious Activity Analysis**

- **Domain**: Website security and risk analysis.
- **Expert**: Cybersecurity analyst.
- **Keywords**: Blacklisted IPs, malicious subnets, SSL certificates.
- **Assumptions**: This area contains potential security vulnerabilities or malicious activities linked to the website.
- **Approach**:
 - Identify any blacklisted or malicious IP addresses and subnets.

- Review SSL certificate information to detect potential mismatches or weaknesses.
- Analyze DNS records to see if there are any security risks.

4. **Website Structure and Content Analysis**

****Domain**:** Website structure and technologies used.

- ****Expert**:** Web development and security expert.
- ****Keywords**:** HTTP headers, web technologies, external and internal URLs.
- ****Assumptions**:** This data provides insight into how the website is built and interacts with external content.
- ****Approach**:**
 - Evaluate the website's HTTP headers for any unusual configurations.
 - Check the web technologies used (e.g., CMS, frameworks) for potential vulnerabilities.
 - Review the external and internal linked URLs to assess security and operational risks.

5. **Geographical and Physical Information Analysis**

****Domain**:** Geographical profiling and site hosting.

- ****Expert**:** Geopolitical analyst.
- ****Keywords**:** Physical addresses, coordinates, country names.
- ****Assumptions**:** The geographical data links the website to specific regions, which may indicate geopolitical relevance.
- ****Approach**:**
 - Analyze the geographical distribution of physical addresses and coordinates.
 - Check for any patterns in hosting locations or connections to specific countries.
 - Identify potential risks based on the country affiliations of servers and affiliates.

I will now perform the analysis for each of these areas starting with ****Affiliate Information**** and move sequentially through all sections.

PIC

PAGE_0003

It appears that the column names in the Excel file differ slightly from what I expected. Let me examine the structure of the dataframes to better understand how the data is organized, and then proceed with the analysis of affiliate information.

It seems that all the affiliate-related sheets have generic column names like `Updated`, `Module`, `Source`, `F/P`, and `Data`. It looks like the actual affiliate data is contained in the `Data` column. I'll now extract and analyze the contents of the `Data` column from each sheet to identify patterns or risks within the affiliate information.

Affiliate Information Analysis

1. ****Company Name**:** The main company mentioned is "VR Systems, Inc.", which appears consistently across the entries. This could be a central affiliate or a primary organization involved with the scanned website.
2. ****Domain Name**:** The domain `domaincontrol.com` is used for all entries. This domain is commonly associated with domain registration and management services, which might indicate that the affiliate domains are registered through this service.
3. ****Email Address**:** Only one email, `server-certs@thawte.com`, is listed. This address is related to Thawte, a certificate authority, likely used for managing SSL certificates.
4. ****Internet Name**:** The sheet lists several internet names, including `bakerelections.com`, `bayvotesfl.gov`, `clayelections.gov`, and others, showing various election-related domains.

Potential Patterns and Risks:

- ****Centralized Control**:** The use of a single company and domain (`VR Systems, Inc.` and `domaincontrol.com`) across multiple entries suggests that a centralized entity manages the domains, which could pose a risk if this entity is compromised.
- ****Certificate Management**:** The presence of Thawte for SSL certificates suggests that security certificates are actively managed, which is positive from a security standpoint.

Networking and Hosting Analysis

P16 PAGE - 0004

From the extracted data, the following key observations can be made:

1. **IP Addresses**: The IP addresses primarily belong to the netblock `3.166.192.0/21` with Amazon Web Services (AWS) as the hosting provider. This indicates that the website scan is associated with cloud infrastructure provided by Amazon.
2. **Netblock Membership**: The netblock `3.166.192.0/21` is associated with AWS, indicating that the scanned website relies on scalable and robust cloud-based infrastructure.
3. **Hosting Provider**: All identified hosting providers are linked to **Amazon AWS**. This is a common choice for high-availability hosting and suggests the website might be using a reliable cloud platform for scalability and security.
4. **BGP AS Membership**: The BGP AS numbers (14618, 16509) are registered to Amazon, confirming the website's reliance on AWS infrastructure for routing internet traffic.

Potential Patterns and Risks:

- **Concentration on AWS**: The use of AWS as the primary hosting provider can be a strong point due to AWS's reliability and security features. However, a single point of failure exists if the AWS service or its network is compromised.
- **Shared Infrastructure**: The common netblock suggests that multiple entities may share the same AWS infrastructure, which could present risks if other entities on the same netblock are compromised.

Security and Malicious Activity Analysis

Here are the key observations from the security-related data:

1. **Blacklisted IPs**: One blacklisted IP, `54.208.31.55`, was flagged by **PhishStats**, suggesting phishing activity associated with this address.

P16 - 006s

PAGE-0005

2. **Malicious IPs**: One IP address, `54.208.31.48`, was identified by **Maltiverse** as being involved in malicious activity, further described as malware-related. Another malicious IP, `54.208.31.55`, was also flagged by PhishStats, showing phishing activity.

3. **SSL Certificates**:

- The issuer for the SSL certificates is **Amazon RSA 2048 M03**, indicating that Amazon provides the certificates.

- Two mismatches were noted:

- One with the domain `clayelections.gov`
- One with the domain `www.voterfocus.com`

These mismatches could be a potential vulnerability, as SSL mismatches might lead to security warnings or a man-in-the-middle attack risk.

Potential Patterns and Risks:

- **Phishing and Malware Activity**: The presence of blacklisted and malicious IP addresses indicates potential threats. These IPs could pose risks if associated with phishing campaigns or malware dissemination.

- **SSL Certificate Mismatches**: SSL mismatches on critical domains such as election-related websites (`clayelections.gov`, `www.voterfocus.com`) could lead to trust issues for users and expose the websites to security vulnerabilities.

Website Structure and Content Analysis

Here are the key observations from the extracted data:

1. **Webserver Headers**: The headers often specify content types such as `application/octet-stream`, `application/x-javascript`, and `text/html`. Additionally, cookies related to session management, mobile views, and analytics are noted. This suggests that the website uses complex server-side processing to deliver dynamic content and track user behavior.

2. **External Links**: The website links to external domains like `dos.myflorida.com` and `dhr.dos.state.fl.us`, which are government-related. This suggests the website interacts heavily with state-level election or government resources.

P16-
PAR - 0006

3. **JavaScript URLs**: JavaScript URLs are predominantly related to election results and information hosted on subdomains like `electionsfl.org`. These scripts are likely responsible for interactive features on the election-related pages.

4. **Target Web Content**: The website seems to use technologies like **jQuery**, with versions such as `1.9.1` and `1.11.4`. While these are widely used, older versions of jQuery can have known vulnerabilities, which should be assessed for potential security risks.

Potential Patterns and Risks:

- **Dynamic Content Handling**: The presence of various content types and session cookies suggests a reliance on dynamic content generation, which could present opportunities for vulnerabilities such as session hijacking if not properly managed.
- **External Dependencies**: The reliance on external governmental resources might make the website more vulnerable if any of these linked resources are compromised or experience downtime.
- **Outdated JavaScript Libraries**: The use of older versions of JavaScript libraries (like jQuery) could introduce security vulnerabilities if they are not regularly updated.

Geographical and Physical Information Analysis

Here are the key observations from the geographical and physical information:

1. **Geoinfo**: The majority of the geographic information points to **Seattle, Washington** (12 entries) and **Philadelphia, Pennsylvania** (4 entries). These locations are commonly associated with large data centers and cloud service providers, particularly Amazon Web Services (AWS). One entry mentions **Ashburn, Virginia**, another key data center location in the U.S.

2. **Physical Addresses**: Two addresses are listed, both linked to Amazon Web Services:

- **410 Terry Ave N., Seattle, WA**
- **Amazon Web Services, Inc., P.O. Box 81226, Seattle, WA**

PTC

PAGE 60007

3. **Physical Coordinates**: Only one set of coordinates is listed, corresponding to a location in Seattle, WA.

Potential Patterns and Risks:

- **Reliance on AWS Data Centers**: The website heavily relies on data centers in Seattle and Philadelphia, which suggests centralization in terms of its hosting infrastructure. While this can ensure high availability, it also poses a risk if there is a regional issue affecting these data centers.
- **Geographical Redundancy**: The presence of multiple geographic locations, particularly major cloud infrastructure hubs, indicates a level of redundancy, which is positive for reliability and security.

Summary of Key Findings:

1. **Affiliate Information**: The data indicates centralized control by VR Systems, Inc., which could be a risk if compromised. Affiliates use domaincontrol.com for registration, and Thawte handles certificates.

2. **Networking and Hosting**: AWS hosts all IP addresses, and there is a reliance on Amazon's cloud infrastructure. This provides scalability but could be a single point of failure.

3. **Security and Malicious Activity**: Blacklisted and malicious IPs are associated with phishing and malware. SSL mismatches on election-related domains pose security risks.

4. **Website Structure and Content**: The site uses dynamic content and links to external government resources. Outdated JavaScript libraries (jQuery) could present vulnerabilities.

5. **Geographical Information**: The site relies on AWS data centers in Seattle and Philadelphia, providing redundancy but centralizing risk in these regions.

P16

PAGE - 0008

Ports Observed:

There are **721 unique open ports** observed in the dataset. Here are a few key examples of ports and their associated functions:

- **Port 443**: This is used for HTTPS (secure web browsing). It ensures encrypted communication between a web browser and the website.
- **Port 1080**: Commonly used for **SOCKS Proxy** connections, enabling the routing of traffic between a client and server.
- **Port 992**: Typically used for **TELNETS**, which is a secure version of the Telnet protocol for communication over a network.
- **Port 995**: Used for **POP3S** (Post Office Protocol 3 Secure), for retrieving emails over SSL.
- **Port 110**: Used for **POP3**, a standard email protocol for receiving emails from a server.

Here is the detailed description of all ports:

Here is a detailed breakdown and explanation of the ports observed in the data, including their common uses and potential security concerns.

Full Breakdown of Common Ports and Their Functions

Port Number	Service/Protocol	Function	Potential Risks
1080	SOCKS Proxy	Used for traffic routing between client and server through a proxy.	If misconfigured, it can be exploited for malicious traffic routing or anonymity for attackers.
992	Telnet over SSL	Provides encrypted remote access using Telnet over an SSL connection.	Telnet is inherently insecure; SSL improves it, but it can still be vulnerable to man-in-the-middle attacks.
995	POP3 over SSL (Secure POP3)	Used for retrieving emails securely from a mail server using SSL encryption.	Generally secure if configured correctly, but SSL/TLS vulnerabilities could affect its encryption.
110	POP3 (Post Office Protocol v3)	Standard protocol for receiving emails from a server, without encryption by default.	Sending unencrypted emails makes it vulnerable to interception, allowing attackers to capture credentials.
80	HTTP (HyperText Transfer Protocol)	Standard web traffic port for unsecured websites.	HTTP traffic is unencrypted, making it vulnerable to man-in-the-middle attacks and data interception.

8/16

Page - 010

443	HTTPS (HyperText Transfer Protocol Secure)	Secure web traffic using SSL/TLS encryption.	Secure if SSL/TLS is configured properly, but misconfigurations or outdated certificates are potential issues.
22	SSH (Secure Shell)	Used for encrypted command-line access and file transfer.	Generally secure, but brute force or weak credential attacks can compromise it.
25	SMTP (Simple Mail Transfer Protocol)	Used for sending emails.	Often used in email phishing, spam distribution, and can be exploited if not secured with proper authentication mechanisms.
53	DNS (Domain Name System)	Used for translating domain names into IP addresses.	DNS poisoning and amplification attacks are common if the DNS server is not properly secured.
21	FTP (File Transfer Protocol)	Used for transferring files between a client and server.	Transmits data in plaintext, including credentials, making it vulnerable to sniffing and interception.
23	Telnet	Used for unencrypted remote access.	Highly insecure, as data (including passwords) is transmitted in plaintext.
3389	RDP (Remote Desktop Protocol)	Used for remote access to Windows machines.	A common target for brute-force attacks, if not secured with strong authentication and encryption.
3306	MySQL Database	Used for connections to MySQL databases.	Unsecured MySQL databases can expose sensitive data; SQL injection attacks are also a concern.

143	IMAP (Internet Message Access Protocol)	Used for retrieving emails, allowing multiple devices to access the same mailbox.	If not encrypted (IMAP over SSL is preferred), email data could be intercepted.
587	SMTP over SSL (Secure SMTP)	Used for sending emails securely with SSL encryption.	If SSL/TLS is not configured correctly, it could introduce vulnerabilities.
993	IMAP over SSL	Secure version of IMAP using SSL encryption.	Secure if SSL is properly configured, but outdated or misconfigured SSL versions may introduce risks.

PI6

PAufz - 011

Analysis and Explanation of the Observed Ports:

1. **Common Web and Email Ports**:

- **Ports 80 (HTTP)** and **443 (HTTPS)** are used for web traffic, with HTTPS being the secure version. Any web services should prioritize using HTTPS to protect users' data and avoid interception.

- **Ports 25 (SMTP)**, **110 (POP3)**, **995 (POP3 over SSL)**, **143 (IMAP)**, and **587 (SMTP over SSL)** are commonly associated with email services. If POP3 or SMTP are used without encryption, emails and credentials are vulnerable to interception.

2. **Security-focused Ports**:

- **Port 22 (SSH)** is used for secure shell access, which is critical for managing servers. However, ~~strong~~ password policies and key-based authentication should be enforced to prevent brute-force attacks.

- **Port 992 (Telnet over SSL)** and **1080 (SOCKS Proxy)** show that the system is using encrypted remote access and proxy services, which can add layers of security but could also be potential points of attack if not properly secured.

3. **Database and Remote Access Ports**:

- **Port 3389 (RDP)** and **3306 (MySQL)** are high-risk if exposed to the internet without proper authentication and encryption. Both are frequently targeted for brute-force attacks or exploitation of vulnerabilities.

4. **Outdated/Insecure Protocols**:

- **Port 23 (Telnet)** and **Port 21 (FTP)** are both outdated and insecure protocols as they transmit data in plaintext. If these are in use, they should be replaced with more secure alternatives like SSH and SFTP.

Security Implications:

- **Unencrypted Services**: Ports like **110 (POP3)**, **23 (Telnet)**, and **21 (FTP)** are unencrypted by default, exposing data to interception and attacks.

- **Remote Access Vulnerabilities**: Ports like **3389 (RDP)** and **22 (SSH)**, while providing necessary functionality, are often targets for brute-force and credential attacks. They should be protected with strong encryption, two-factor authentication, and IP filtering.

P19 PAGE 001

Analysis of VRsystems.com

1. Domain Structure and Hosting

- Subdomains and CNAMEs: VR Systems uses several subdomains hosted across third-party platforms like Amazon Web Services (AWS), Google, and Short.io for content delivery, email security, and link tracking. Some examples include:

- `link.vrsystems.com` uses Short.io for URL shortening and redirects.
- `videos.cdn.vrsystems.com` and `mta-sts.vrsystems.com` rely on AWS CloudFront for video hosting and secure email delivery.
- `texas.vrsystems.com` is hosted via AWS Elastic Load Balancer for high traffic.
- GoDaddy is used for DNS management.

1

- Recommendations:

1. Monitor third-party services regularly for vulnerabilities, especially platforms like Short.io, which are commonly targeted for phishing.
2. Conduct regular security audits to ensure configurations on AWS and GoDaddy follow security best practices.

2. IP Address Analysis

- Key AWS IP Blocks: VR Systems heavily depends on AWS, as shown by the presence of multiple AWS IP ranges, including those flagged for blacklisting by CleanTalk and VoIPBL. Some of these include:

- `54.208.0.0/15` flagged for spam and phishing activities.
- Other AWS IPs like `54.208.31.55` flagged by PhishStats for phishing.

- Risks: The blacklisted IPs can harm VR Systems' reputation and impact service delivery, particularly email-related services.

- Recommendations:

1. Immediate investigation into blacklisted IPs and potential phishing activities.
2. Request delisting of wrongly flagged IPs and enhance monitoring with AWS GuardDuty and CloudTrail.

Page 002

3. Implement additional security measures like SPF, DKIM, and DMARC for email systems to protect against spoofing and phishing.

3. Web Infrastructure and Content Delivery

- Web Technologies: VR Systems uses outdated frameworks like Bootstrap 3.3.5 for web design, which may expose vulnerabilities. It also uses Google services for their calendar and Google reCAPTCHA for bot prevention.

- Recommendations:

1. Upgrade to Bootstrap 4 or 5 to mitigate security risks.
2. Regularly review external script dependencies (e.g., Typekit, Google reCAPTCHA) for vulnerabilities.
3. Implement a Content Security Policy (CSP) to prevent cross-site scripting (XSS) attacks.

4. Email Security

- MTA-STS Setup: VR Systems has configured Mail Transfer Agent Strict Transport Security (MTA-STS) to secure email communications, which is a good security practice. However, email-associated IPs have been flagged in some blacklists.

- Recommendations:

1. Continue using MTA-STS for email security, but monitor email server logs for potential breaches.
2. Consider implementing DNSSEC to further secure email transmissions.

5. External Links and Services

- Short.io & Social Media Integration: VR Systems uses Short.io for link tracking, along with Facebook and LinkedIn for marketing. External dependencies, like Google reCAPTCHA, pose a security risk if compromised.

- Recommendations:

1. Secure URL shorteners and limit exposure by implementing two-factor authentication (2FA) or strict access controls.
2. Ensure that social media and tracking pixels do not expose sensitive data.

6. Security Considerations for Cloud and On-Premise Infrastructure

P17

PAGE - 003

- AWS Usage: Heavy reliance on AWS for scalable cloud services, but risks arise from shared infrastructure and potential blacklisting.

- On-premise Servers: The 199.44.96.130 IP address is hosted outside of AWS and may represent on-premises infrastructure.

- Recommendations:

1. Strengthen access control policies for AWS resources, including use of IAM roles.
2. Secure communication between AWS-hosted and on-premises servers using VPN or AWS Direct Connect.

7. Vulnerability and Exposure Risks

- Potential for Exploits: VR Systems exposes several critical services like SSH (port 22), RDP (port 3389), and MySQL (port 3306), which are commonly targeted in attacks.

- Recommendations:

1. Harden SSH with multi-factor authentication (MFA) and key-based access.
2. Restrict database and RDP port access to trusted IP ranges and VPN tunnels.
3. Regularly patch all systems and services to close known vulnerabilities.

8. Blacklisted IP and Fraudulent Activities

- PhishStats and CleanTalk: Some of VR Systems' IPs are flagged for phishing and spam activities, particularly the 54.208.x.x AWS block.

- Recommendations:

1. Block and monitor traffic to and from flagged IPs.
2. Request delisting of blacklisted IPs and investigate potential misuse.

9. Critical Infrastructure Exposure

- Critical Subdomains: Subdomains like deploy.vrsystems.com and tempest.vrsystems.com could expose sensitive development or testing environments.

- Recommendations:

1. Restrict access to critical subdomains, especially for deployment environments, and ensure strong authentication.

2. Regular vulnerability scans to detect any exposed services or misconfigurations.

10. Recommendations for Future Action

- Conduct Regular Security Audits: Across all AWS-hosted services, on-premises infrastructure, and externally exposed systems.
- Implement Monitoring and Incident Response: Use tools like AWS CloudTrail, GuardDuty, and Security Hub to monitor for potential threats and respond quickly to incidents.
- Reinforce Backup and Redundancy: Ensure that all election-related services have localized backup systems in case of service disruptions or attacks.

Conclusion

VR Systems demonstrates robust cloud-based infrastructure, but there are significant security risks that need to be addressed to maintain operational integrity. Immediate focus should be on blacklisted IP remediation, third-party service monitoring, securing critical subdomains, and enhancing security around exposed services such as SSH and MySQL.

By addressing these vulnerabilities and implementing the recommendations, VR Systems can greatly reduce its risk profile and ensure secure, scalable, and resilient service delivery.

Subdomains and CNAMEs:

1. link.vrsystems.com → CNAME record pointing to `short.io`:

- This suggests that the `link.vrsystems.com` subdomain is being managed through a URL shortening or redirecting service, `short.io`. This could be used for tracking, marketing, or external link management.

2. videos.cdn.vrsystems.com → CNAME record pointing to `d1xmibnic3bahh.cloudfront.net`:

- This subdomain is using Amazon CloudFront, a content delivery network (CDN), to host videos. The use of CloudFront helps improve performance by caching content across different geographic locations.

3. mta-sts.vrsystems.com → CNAME records pointing to CloudFront (`d36xwd7stvtot8.cloudfront.net`) and various AWS DNS servers:

- `mta-sts` is related to Mail Transfer Agent Strict Transport Security, which is a protocol used to ensure secure email delivery. The DNS records indicate that the domain is using AWS infrastructure to handle this securely.

4. texas.vrsystems.com and www.texas.vrsystems.com → CNAME records pointing to `dnnredireceter-910902575.us-east-1.elb.amazonaws.com`:

- These subdomains seem to be redirecting through an Elastic Load Balancer (ELB) in AWS. This indicates that the Texas-related subdomains are hosted on AWS, possibly handling high traffic or regional operations.

5. calendar.vrsystems.com → CNAME pointing to `ghs.google.com`:

- This is likely associated with Google Apps (Google Calendar), indicating that VR Systems uses Google services to manage their calendar system through this subdomain.

6. vrsystems.com → Name servers from GoDaddy (ns51 and ns52.domaincontrol.com):

- The primary domain uses GoDaddy for its DNS management. This is a common choice for domain management, indicating that the root domain is registered and controlled via GoDaddy.

7. www.vrsystems.com → CNAME record pointing to `tlh.corp.vr2838.net`:

- The primary website 'www.vrsystems.com' redirects to a corporate network ('vr2838.net'), possibly indicating internal hosting or legacy infrastructure for the web application.

General Observations:

- AWS Infrastructure: Many of the subdomains are hosted using AWS services (Elastic Load Balancers, CloudFront, AWS DNS), which points to a strong reliance on cloud-based infrastructure for content delivery, email security (MTA-STS), and regional routing (e.g., Texas subdomains).

- Google Services: The 'calendar.vrsystems.com' subdomain is leveraging Google services, which may indicate the usage of Google Workspace for their internal productivity tools.

- Short.io for Redirection: The 'link.vrsystems.com' subdomain uses 'short.io', which may suggest external link tracking or redirection. This could pose a potential attack vector if not properly secured, as URL shorteners can sometimes be abused for phishing.

Security and Vulnerability Considerations:

1. Email Security (MTA-STS): The presence of MTA-STS indicates a concern for email security and mitigation of MITM (man-in-the-middle) attacks during email delivery, which is a positive sign.

2. Potential Third-Party Dependencies: The use of multiple third-party services (AWS, CloudFront, Google, Short.io) introduces potential risks, especially if these services are not kept secure or are vulnerable to attacks. It's important to ensure that proper configurations and security best practices (e.g., strict CNAME delegation) are followed.

3. Cloud and Load Balancing: The heavy use of AWS for hosting via CloudFront and ELB (Elastic Load Balancer) indicates that VR Systems is relying on scalable cloud infrastructure, which can help in handling traffic and redundancy. However, it's essential to ensure that proper security policies (like IAM, security groups, SSL configurations) are enforced to avoid common cloud misconfigurations.

4. Corporate Subdomain Redirects: The 'www.vrsystems.com' redirect to 'vr2838.net' suggests internal infrastructure that might not be exposed externally. However, this should be investigated further to ensure that the corporate network is properly segmented from any public-facing services.

Affiliated IP Addresses

P11- Page 007

The analysis of the affiliate IP addresses gathered using Spiderfoot shows a list of adjacent IP addresses (neighbors) associated with the domain 'vrsystems.com'. This information highlights IP address blocks and hosting services being used. Below is a detailed breakdown of the findings and potential insights from this data:

Key IP Blocks and Their Significance

1. 18.205.213.x Block:

- These IPs belong to Amazon Web Services (AWS), specifically part of the EC2 instance blocks in the U.S. East region.
- Multiple adjacent IP addresses (192-207) suggest that the systems or services hosted on 'vrsystems.com' rely on AWS infrastructure, likely for scalable web hosting, data processing, or content delivery.
- This block indicates a strong reliance on cloud services, which is typical for modern web applications.

2. 199.44.96.x Block:

- The IP range (128-143) seems to be associated with a different hosting service provider. This block may belong to another data center or private infrastructure being used by VR Systems for specific services.
- Having these addresses adjacent to each other could indicate that this block is reserved for specific application services or managed infrastructure.

3. 23.23.80.x Block:

- This range is also associated with AWS. The specific range (192-207) falls within the Elastic IPs used for various AWS services.
- Similar to the 18.x block, this highlights AWS usage, but it may serve different regions, applications, or services for VR Systems.

4. 34.202.217.x Block:

- Another AWS block, part of the U.S. East region. These IPs (64-79) are part of the larger AWS network likely used for VR Systems' cloud-hosted applications and services.

PT

PAGE - 008

- It appears that various parts of VR Systems' infrastructure are deployed across multiple AWS IP ranges, ensuring distributed and resilient service.

5. 52.22.23.x Block:

- Another range hosted on AWS, covering IPs from 128 to 143. This is further evidence that AWS hosts significant portions of the VR Systems infrastructure, with multiple Elastic IPs distributed across services.

6. 54.157.233.x Block:

- This block (240-255) is part of AWS as well. These IPs might be associated with load balancers, specific web applications, or cloud storage services.
- This continuous range again indicates extensive use of AWS for the domain.

7. 65.9.149.x Block:

- This is a different type of block, likely related to Amazon CloudFront (AWS's CDN service). The wide range of adjacent IPs suggests that VR Systems may be using CloudFront for content distribution and caching, which is beneficial for delivering web content faster and more reliably across regions.
- IPs in the range of 0-95 highlight a significant allocation of IPs, pointing to possibly large-scale or globally distributed operations.

General Observations and Potential Insights:

- Reliance on AWS: The majority of the IP blocks in this analysis belong to AWS, which indicates that VR Systems is heavily dependent on Amazon Web Services for its infrastructure. This is common for organizations that require scalable, secure, and high-availability cloud hosting for applications, websites, and data storage.
- Content Distribution: The presence of CloudFront (65.9.x.x) IPs suggests that VR Systems uses Amazon's CDN to optimize the delivery of web content to its users. This would improve website performance and load times for users across different geographic regions.

017 PAGE-009

- Distributed IP Allocation: The allocation of IPs in different AWS blocks across various ranges (18.x, 23.x, 34.x, 52.x, 54.x) indicates a distributed infrastructure setup. This suggests that VR Systems could be using load balancing, failover systems, or region-specific hosting to maintain uptime and service availability.
- Multiple Hosting Providers: While AWS seems to be the dominant provider, there are signs that other hosting infrastructures may be in use (such as the 199.x block). This could either be legacy infrastructure or a secondary hosting provider used for specific purposes like backup or specialized services.

P19-

PAGE-010

The data provided from Tab 4 and Tab 5 shows that some IP addresses and ranges affiliated with the `vrsystems.com` domain have been flagged on various blacklists. Here's a breakdown of the information from both tabs, along with the potential implications and recommendations.

Tab 4: Blacklisted IP Address on PhishStats

- IP Address: `54.208.31.55`
- Blacklist Source: PhishStats
 - Description: PhishStats tracks phishing campaigns and related malicious activities. The IP address `54.208.31.55` has been flagged in this context.
 - Implications: This indicates that one of the IP addresses within the AWS infrastructure that VR Systems is using has been involved in a phishing campaign, whether directly or indirectly. It's possible that this was a result of a compromised service, misconfiguration, or shared AWS IPs being used for malicious purposes by another tenant on the same network.

Tab 5: Blacklisted IP Range in Multiple Blacklists

1. IP Range: `54.208.0.0/15`
 - Blacklist Source: CleanTalk Spam List
 - Description: CleanTalk is a widely used spam filtering service that maintains a list of IP addresses associated with spam activities. The presence of the `54.208.0.0/15` range on this list suggests that either VR Systems or another tenant sharing the same AWS infrastructure may have been involved in spamming activities.
 - Implications: This could affect VR Systems' reputation, especially if they send emails or interact with services that rely on spam filtering to block unwanted content.
2. Blacklist Source: VoIP Blacklist (VoIPBL)
 - Description: VoIPBL is a project that tracks IP addresses involved in VoIP (Voice over IP) abuse, typically to identify those used in scams or illegal operations involving VoIP services. The entire `54.208.0.0/15` block is listed here.
 - Implications: If VR Systems uses VoIP services for customer support, internal communications, or other purposes, being on this blacklist could lead to communication disruptions or reputational damage. Even if VR Systems is not directly involved, other users of the AWS range may have triggered the listing.

P17

PAGE 011

Analysis and Potential Impacts:

1. Reputation Risks: The presence of these IPs and ranges on blacklists can affect VR Systems' reputation, especially in terms of email deliverability, phishing prevention, and interaction with external systems that rely on these blacklists for security. Other organizations may block or limit interactions with VR Systems' infrastructure, thinking it's compromised or being used for malicious activities.
2. AWS Shared Infrastructure: Since these IPs are part of the AWS infrastructure, it's possible that VR Systems is not directly responsible for the malicious activities. AWS shares its IP space among many customers, and if one customer is compromised or engaged in bad behavior, it can affect others using the same IP range. This underscores the importance of maintaining good standing with cloud providers and promptly addressing any security or compliance issues.

Recommendations:

1. Investigate the Blacklisted IPs: VR Systems should immediately investigate whether their services are being directly affected or compromised, especially in the case of the phishing-related flag on PhishStats. This could involve:
 - Reviewing security logs for any abnormal activity associated with '54.208.31.55'.
 - Checking for any potential phishing attempts or email-based attacks originating from their infrastructure.
 - Verifying whether the IPs in question are indeed assigned to their services or shared with other AWS tenants.
2. Request Delisting: If it is determined that VR Systems is not responsible for the blacklisted activities, it may be possible to request delisting from these blacklists. For the CleanTalk Spam List and VoIPBL, VR Systems can use the provided URLs to check the status and follow up on removal:
 - [CleanTalk Spam List](https://iplists.firehol.org/files/cleantalk_7d.ipset)
 - [VoIPBL Check](<https://voipbl.org/check/?ip=54.208.0.0/15>)
3. Harden Security Posture:
 - Email Security: Implement measures like SPF, DKIM, and DMARC for outgoing email, ensuring email security standards are followed to avoid being flagged as spam.

PM

Page - 012

- Monitoring and Incident Response: Increase monitoring for any potentially suspicious or malicious activities within their AWS-hosted services, using tools such as AWS CloudTrail and AWS GuardDuty to detect anomalies.

- Segregate Sensitive Services: If VR Systems relies on critical services like VoIP or email, consider using a dedicated IP range or email service that ensures separation from potentially blacklisted IPs shared by other AWS customers.

4. Communicate with AWS Support: Reach out to AWS support to notify them of the issue and inquire about any additional steps AWS can take to ensure that VR Systems is not affected by blacklisting caused by other tenants sharing the same IP space.

By addressing these blacklisted IPs promptly and implementing security measures, VR Systems can protect its infrastructure from further reputational damage and operational disruptions.

PH

PAR - 013

The data provided in this tab appears to represent HTML metadata and page structure information for various sections of the VR Systems, Inc. website, detailing content such as news and events, products, customer testimonials, and privacy policies. This information is useful in gaining insights into the structure, content, and setup of the website. Here's a breakdown of the analysis:

Key Points:

1. Consistent Use of HTML Metadata:

- Each page contains standard HTML metadata tags, such as 'MetaDescription', 'MetaKeywords', and 'MetaRobots'. These are important for SEO (search engine optimization) and controlling how search engines index the site.
- The pages consistently have '<meta>' tags for revisiting frequency (1 day), which suggests an attempt to keep content fresh and encourage frequent indexing by search engines.

2. Responsive Design and CSS:

- The website uses several stylesheets ('dnndefault', 'bootstrap', and custom styles) that appear to ensure responsive design across devices, with references to bootstrap 3.3.5. This is somewhat outdated, as newer versions of Bootstrap have been released, and using older frameworks may present compatibility or security concerns.
- The 'skin.css' and other VR-branded stylesheets help in creating a consistent branding and user experience across the website.

3. Page Titles:

- The titles are descriptive and SEO-friendly, such as:
 - "VR Systems Inc. > Our Customers > Testimonials"
 - "VR Systems Inc. > Solutions > Electronic Pollbook"
- These are properly formatted for each page, following a structured hierarchy to improve search engine rankings.

4. Page Content and Structure:

- The website covers a wide range of content, including product offerings (e.g., Electronic Pollbooks, VR Tower, Voter Focus), news, events, and white papers.

P17 PAGE - 014

- The website contains sections dedicated to customer resources, such as testimonials, white papers, and requests for demos. This supports the company's focus on providing solutions and customer education.

5. Focus on Elections Technology:

- The pages reflect a clear emphasis on elections-related technology, including solutions for election management, voter registration, and online training platforms.
- The repeated use of keywords like "election," "voter," and "electronic pollbook" indicates a strategic alignment with their core business focus, which is serving election infrastructure needs.

6. Security and Compliance Considerations:

- The website's use of HTTPS (as indicated by the use of URLs referencing "https://maxcdn.bootstrapcdn.com/") shows a good practice for securing content delivery. However, the reliance on older frameworks like Bootstrap 3.3.5 might need to be reviewed to ensure that any potential security vulnerabilities are addressed.

Potential Issues and Recommendations:

1. Outdated CSS Framework:

- The use of Bootstrap version 3.3.5 indicates the website may not be up-to-date with the latest web development standards. Bootstrap 3 has known vulnerabilities and lacks modern features compared to Bootstrap 4 or 5. Upgrading the framework would enhance both security and user experience.

2. SEO Optimization:

- While the pages include necessary SEO tags like 'MetaKeywords' and 'MetaDescription', some tags are relatively generic (e.g., "Election, Voter, Pollbook"). Consider updating these tags to better reflect unique page content for more targeted search engine optimization.

3. Meta Revisit Tag:

- The use of the `<meta name="REVISIT-AFTER" content="1 DAYS">` tag is obsolete in modern SEO practices. Search engines like Google no longer respect this tag. VR Systems might want to update or remove this tag to modernize their site's SEO.

P17-

PAbh-015

4. Consistency and Usability:

- The website appears to be consistently structured, and there's a strong focus on user navigation through clear page titles like "Request a Demo," "News and Events," "Products," etc. This helps visitors easily find information relevant to them.
- Testing the website for usability across modern browsers and devices is recommended to ensure that the design remains responsive and fully functional.

5. Website Performance and Optimization:

- The inclusion of multiple CSS files could lead to increased load times, especially if not optimized. Consider combining or minimizing these CSS files to improve page performance.

P17-

PAGE - 016

The data provided in this tab lists connected domains, primarily election-related government websites, along with their origin country. All of the domains listed are from the United States, indicating they are local election offices or organizations connected to election systems, likely through partnerships with VR Systems, which provides critical election infrastructure, including election night reporting and election staff training.

Key Observations:

1. Geographic Focus:

- The domains all point to U.S.-based election offices, predominantly in Florida, as indicated by the "fl" in many domain names (e.g., 'votebradfordfl.gov', 'votecolumbiafl.gov', etc.).
- VR Systems appears to have significant connections or provide services to multiple county-level election offices across the U.S., with a notable concentration in Florida, a critical state in U.S. elections.

2. Nature of Domains:

- Many of these domains (e.g., 'voteokaloosa.gov', 'votemarion.gov') are official government websites responsible for election-related services, such as voter registration, reporting election results, and sharing public information on voting procedures. These domains generally belong to the county Supervisors of Elections.
- The '.gov' top-level domain (TLD) signifies verified U.S. government entities, confirming these are official and trusted sources for election services.

3. VR Systems' Role:

- VR Systems is likely providing election night reporting systems and staff training to these counties. This suggests that VR Systems' services play a critical role in ensuring real-time reporting of election results and adequately preparing election workers to handle voting procedures.

- The large number of connected domains shows VR Systems' extensive involvement in supporting county-level election infrastructure, especially in Florida, where accurate and efficient election operations are crucial.

Security and Reliability Considerations:

1. Centralized Service Provider:

P17

PAGE- 017

- With VR Systems serving as a centralized provider for election reporting and staff training, it's vital that they maintain rigorous security protocols. Any breach could disrupt election night reporting or compromise the training systems that are essential for staff readiness during elections.

2. Trust and Integrity:

- The '.gov' domains provide a high level of trust due to their government affiliation. However, being closely tied to election reporting and staff training systems makes these domains potential high-value targets for malicious actors. It's critical that VR Systems ensures these systems are protected from cybersecurity threats to maintain the integrity of the elections.

3. Risks of Centralization:

- The centralization of critical services like election night reporting and staff training under VR Systems poses potential risks. A security vulnerability or system failure at VR Systems could have widespread implications across multiple counties. Robust disaster recovery plans and cybersecurity measures are necessary to mitigate these risks and ensure uninterrupted election operations.

Recommendations:

1. Security Audits:

- Regular security audits and penetration testing are essential to ensure that VR Systems' infrastructure, especially its election night reporting and staff training systems, are resilient against potential cyberattacks.

2. Localized Backup Strategies:

- County election offices should work with VR Systems to implement localized backup systems for election reporting and training resources. This would reduce dependency on centralized infrastructure and ensure continuity in the event of service disruptions.

3. Incident Response Planning:

- Both VR Systems and its connected election offices should have well-defined incident response plans in place. These plans should address potential cybersecurity threats and outline procedures for quickly addressing any system failures, breaches, or data compromises.

P17

PACR - 018

This data provides insights into the IP addresses and geographic locations associated with various interactions involving election-related systems, specifically connected to VR Systems and other key entities. The records highlight the movement of data and system communications across different regions in the U.S. and some international locations. Here's a breakdown of the analysis:

Key Insights:

1. Concentration in U.S. Data Centers:

- A significant number of the IP addresses are associated with Ashburn, Virginia—a major hub for data centers and cloud services in the U.S. Several large tech companies, including Amazon Web Services (AWS), operate from Ashburn, which suggests that some of these IPs are likely cloud-hosted services supporting election-related infrastructures.

- Other U.S. locations include Boydton, Virginia, Claymont, Delaware, Monroe, Louisiana, and Seattle, Washington. These cities also host major data centers, which implies that election-related data and services are being routed through prominent cloud infrastructure locations.

2. Presence of IPv6 Addresses:

- Many of the IP addresses are in the IPv6 format, which signifies modern infrastructure use. The dominance of IPv6 addresses, particularly from Seattle, Washington, reflects the ongoing transition to the newer IP version, indicating that the connected services are running on up-to-date and scalable internet architectures.

3. Geolocation of International IPs:

- A notable discovery is the appearance of IP addresses from Santiago de Queretaro, Mexico (e.g., '65.9.149.5', '65.9.149.125'). These IPs could represent content distribution networks (CDNs) or other cloud service providers operating internationally, routing global data for optimized service. Given that CDNs often rely on geographically distributed networks, the presence of these IPs suggests global service provisioning for enhanced performance or redundancy.

4. Potential Cloud Service Providers:

- The IP addresses in Ashburn, Virginia, and Seattle, Washington, are consistent with large cloud platforms like AWS, Microsoft Azure, or Google Cloud, which likely host VR Systems'

P17

PARF - 019

services. The involvement of major cloud service providers indicates a reliance on these platforms for handling the scalability and reliability of election-related infrastructure.

5. Data Security Implications:

- The widespread geographic distribution of the IP addresses reflects the complexity of modern election systems that rely on cloud infrastructure across various regions. This geographic distribution suggests potential challenges in securing these systems as data flows across multiple jurisdictions and providers.

6. Regional Focus on U.S. Elections:

- While the data shows connections to international locations (Mexico), the primary focus remains on U.S.-based infrastructure. This suggests that these systems are likely focused on managing U.S. election data or services, but potentially involve CDNs or international backups to ensure data resilience and faster access.

The data you've provided outlines an extensive series of domain and subdomain discoveries related to VR Systems using different DNS-related modules (DNS Brute, DNS Resolve, CRT, and SSL Cert) from a tool like SpiderFoot.

Key Observations:

1. Domain Enumeration:

- The tool has found multiple subdomains of vrsystems.com including key subdomains such as:
 - `calendar.vrsystems.com`
 - `link.vrsystems.com`
 - `videos.cdn.vrsystems.com`
 - `mta-sts.vrsystems.com`
 - `tempest.vrsystems.com`
 - `deploy.vrsystems.com`
 - `www.texas.vrsystems.com`
- These subdomains appear to have distinct functionalities, for instance, calendar, content distribution, mail exchange (mta-sts), and deployment systems.

2. SSL Certificates:

Part - 020

- The presence of Let's Encrypt SSL certificates for several of these subdomains, including:
 - `tempest.vrsystems.com`
 - `link.vrsystems.com`
 - `www.texas.vrsystems.com`
- These SSL certificates are active and have validity periods, mostly from August to November 2024, indicating that they are recent and likely in current use.

3. CloudFront & AWS Association:

- Several subdomains resolve to Amazon CloudFront (e.g., `videos.cdn.vrsystems.com`, `mta-sts.vrsystems.com`), indicating that VR Systems uses Amazon Web Services (AWS) for content delivery and mail services, especially for subdomains dealing with CDN and email services.

4. Subdomain Services:

- `tempest.vrsystems.com` appears to be a significant service, as it is repeated frequently in the analysis, suggesting that it may serve a core function, possibly in deployment, security, or testing environments.
- `www.texas.vrsystems.com` likely relates to election management for the state of Texas, as the naming suggests, and may be state-specific infrastructure provided by VR Systems.

5. DNS Resolutions:

- DNS resolutions for several subdomains show connections to infrastructure like short.io (used for link shortening) and CloudFront, implying that VR Systems is leveraging cloud services to support various parts of their platform.

Analysis of Potential Risks:

- Use of Public Cloud (AWS CloudFront):

- The use of AWS CloudFront for subdomains like `videos.cdn.vrsystems.com` and `mta-sts.vrsystems.com` shows that VR Systems relies on a third-party provider for content delivery and email security. This introduces the potential for dependency risks, but also shows they are using a well-known, scalable, and secure platform.

- Wildcard SSL Certificates:

P17

PART-02

- The presence of Let's Encrypt certificates with relatively short expiration periods suggests that the organization is actively managing its security certificates. However, regular renewal is required to avoid service disruptions.

- Subdomain Exposure:

- The exposure of critical subdomains, such as `deploy.vrsystems.com` (potentially used for development or staging environments), could represent a security risk if improperly secured. If these environments are accessible publicly, they could become targets for attackers.

- Redundancy and Overuse of '`tempest.vrsystems.com`':

- The frequent occurrence of '`tempest.vrsystems.com`' in the analysis indicates that this subdomain may play a critical role. However, any vulnerabilities associated with this subdomain could lead to cascading issues across the VR Systems infrastructure.

Recommendations:

1. Harden Critical Subdomains:

- Ensure that sensitive subdomains like '`deploy.vrsystems.com`' are well-protected with appropriate authentication measures, rate-limiting, and possibly restricted access.

2. Monitor SSL Certificate Renewals:

- VR Systems should continue managing its SSL certificates proactively, with a focus on monitoring upcoming expiration dates to avoid any service interruptions.

3. Regular Audits of Cloud Services:

- Conduct regular audits of services hosted on third-party infrastructure like AWS CloudFront to ensure that security configurations (e.g., encryption, access controls) meet internal and regulatory standards.

4. Subdomain Monitoring:

- Continued monitoring of subdomains for exposure or potential vulnerabilities is necessary, especially for state-specific services like '`texas.vrsystems.com`' and others related to election management.

P17

PAGE -022

In summary, VR Systems is using modern infrastructure with cloud services and active SSL management, but exposure of critical subdomains like 'deploy' and the heavy reliance on AWS for content delivery should be carefully monitored and secured to prevent any exploitation.

Analysis of the IPv6 Addresses Associated with VR Systems

The data you've provided lists multiple IPv6 addresses associated with subdomains and services of VR Systems, which have been resolved through DNS lookups.

Key Insights:

1. Common IPv6 Prefix:

- Almost all IPv6 addresses share a common prefix of 2600:9000:20d1. This prefix suggests that these addresses are part of the same broader network block, most likely allocated by Amazon Web Services (AWS). The remaining suffixes represent the individual subdomains and services.

2. AWS CloudFront Integration:

- The IPv6 addresses are associated with services that rely heavily on AWS CloudFront, such as:

- `d1xmibnic3bahh.cloudfront.net`
- `d36xwd7stvtot8.cloudfront.net`
- CloudFront is Amazon's content delivery network (CDN), which suggests that VR Systems uses this CDN for scaling and delivering content globally, likely for multimedia (videos, content delivery, etc.) and email services.

3. Subdomains & Corresponding IPv6 Addresses:

- Several subdomains, such as mta-sts.vrsystems.com and videos.cdn.vrsystems.com, are resolved to multiple IPv6 addresses. This redundancy is beneficial as it enhances load balancing and ensures reliability in case of network issues with any one address.

- Notably:

PM

PAUL 023

- mta-sts.vrsystems.com is an email-related service, using IPv6 addresses like `2600:9000:20d1:1000:2:c2ad:7700:93a1` and others.
- videos.cdn.vrsystems.com is resolved to multiple addresses (`2600:9000:20d1:a00:8:fb9f:3540:93a1`, among others), indicating a content distribution service.

4. Wide Geographic Distribution:

- The repetition of IPv6 addresses across different subdomains is indicative of the fact that AWS CloudFront is utilizing a globally distributed infrastructure. By routing to multiple IPv6 addresses, VR Systems ensures optimized content delivery with minimal latency.

5. Use of MTAs and STS for Email Security:

- The subdomain mta-sts.vrsystems.com indicates that VR Systems is employing MTA-STS (Mail Transfer Agent Strict Transport Security), which is designed to secure email transmissions by enforcing TLS encryption and preventing downgrade attacks. This enhances the email security of VR Systems, ensuring that their communications are protected from interception or tampering.

6. Repetition and Redundancy:

- Many of the IPv6 addresses are repeated across different services, which implies redundancy for high availability. For instance, mta-sts.vrsystems.com resolves to several IPv6 addresses, allowing for reliable email transport and fallback mechanisms in case one address or route fails.

Security Considerations:

1. IPv6 Addressing in Cloud Services:

- The extensive use of IPv6 by VR Systems, especially with AWS CloudFront, showcases a modern infrastructure that is capable of handling high traffic and global distribution. However, VR Systems should ensure that all access to these services, especially those related to sensitive data like email (via MTA-STS), is tightly controlled with proper authentication and encryption.

2. MTAs and DNS Security:

PCT

PA5E-024

- The presence of `mta-sts.vrsystems.com` reflects VR Systems' proactive approach to email security. However, they should also implement DNSSEC to further protect against DNS spoofing or interception attempts.

3. Content Delivery and Reliability:

- The use of CloudFront IPv6 addresses for videos.cdn.vrsystems.com shows that VR Systems is focused on scaling content delivery. It's crucial to monitor and manage the content being served through these addresses to avoid security vulnerabilities or accidental exposure of sensitive content.

Recommendations:

1. Monitor IPv6 Addresses:

- VR Systems should continue monitoring the IPv6 addresses used for these services, ensuring there are no rogue or unmonitored IP addresses in use. Regular audits of cloud infrastructure should be conducted.

2. Optimize Load Balancing & Redundancy:

- While redundancy is in place, ensure load balancing mechanisms are optimized to distribute traffic evenly across all available IPv6 addresses, preventing any single point of failure or service degradation.

3. Implement Additional Security Layers:

- Strengthening the security around services exposed via IPv6, especially content distribution and email (MTA-STS), can be achieved through advanced security mechanisms like DNSSEC, IP reputation monitoring, and ensuring that traffic encryption (TLS) is enforced across all endpoints.

Conclusion:

The IPv6 addresses discovered in relation to VR Systems suggest a robust cloud infrastructure leveraging AWS CloudFront for content delivery and secure email communications. The widespread use of IPv6, coupled with MTA-STS for email security, shows a modern and scalable infrastructure. However, continuous monitoring and the application of additional security layers will help safeguard against any potential threats or disruptions.

PAGE - 025

Analysis of the IPv4 Addresses Associated with VR Systems

The data you've provided lists IPv4 addresses associated with various subdomains and services of VR Systems. Here's an analysis of these IP addresses, their potential roles, and related services.

Key Insights:

1. Amazon Web Services (AWS) Integration:

- Many of the IPv4 addresses in this list are associated with AWS infrastructure, which indicates that VR Systems relies heavily on AWS for hosting and content delivery. For instance:

- `34.202.217.71` and `54.157.233.240` are used by both `texas.vrsystems.com` and `www.texas.vrsystems.com`, pointing to AWS-hosted infrastructure, possibly in the US East region (Northern Virginia).

- `mta-sts.vrsystems.com` resolves to multiple IP addresses in the range `65.9.149.x`, which are part of AWS's CloudFront service. CloudFront is typically used for scaling services globally, enhancing performance, and delivering secure content, as well as email services in this case.

2. Email Security with MTA-STS:

- The `mta-sts.vrsystems.com` subdomain resolves to several AWS CloudFront IP addresses, such as:

- `65.9.149.119`, `65.9.149.5`, `65.9.149.55`

- These IPs are part of VR Systems' MTA-STS (Mail Transfer Agent Strict Transport Security) implementation, which enhances email security by enforcing TLS encryption for email transmissions, ensuring that VR Systems communications remain secure.

3. Custom Subdomains Hosted on AWS:

- Subdomains such as `tempest.vrsystems.com` (23.23.80.199) and `deploy.vrsystems.com` (52.177.184.148) are also hosted on AWS, further confirming that AWS plays a significant role in VR Systems' infrastructure.

00

PAGE - 026

- '23.23.80.199' belongs to AWS's EC2 instances, which suggests that tempest.vrsystems.com is being served from a cloud-based virtual machine, while '52.177.184.148' indicates another AWS-hosted service.

4. Mixed Hosting with On-Premises Servers:

- One address stands out as non-AWS and is likely hosted outside of AWS:
 - tlh.vrsystems.com resolves to '199.44.96.130', which appears to be hosted on a different infrastructure. This could be an on-premises server or hosted through another cloud provider or colocation facility. This address likely serves localized content or internal services.

5. Content Delivery Network (CDN) for Video Services:

- The subdomain videos.cdn.vrsystems.com resolves to multiple IPv4 addresses ('65.9.149.x'), all of which belong to AWS CloudFront. These IPs indicate that VR Systems is using CloudFront's CDN to deliver video content efficiently to users, which helps in improving load times and reducing latency globally.

6. Multiple IP Resolutions for High Availability:

- Several subdomains resolve to more than one IP address, ensuring redundancy and load balancing:
 - For example, texas.vrsystems.com resolves to both '34.202.217.71' and '54.157.233.240'. This setup improves availability and distributes traffic across multiple servers, ensuring the service remains available even if one server goes down.

7. Legacy Systems or Different Providers:

- link.vrsystems.com resolves to '207.174.61.1', which might belong to a different hosting provider or legacy infrastructure. This could be part of an older setup, or a service hosted outside AWS. It's important for VR Systems to manage and secure these separate infrastructure components effectively, ensuring they integrate securely with the rest of the AWS-hosted systems.

Security Considerations:

1. AWS Security Best Practices:

P17

PAGE 027

- VR Systems' reliance on AWS CloudFront for services such as mta-sts, video delivery, and custom subdomains is a modern and scalable choice. However, strict security measures must be enforced, such as:

- Implementing AWS Shield and AWS WAF (Web Application Firewall) to prevent DDoS attacks.
- Utilizing IAM roles with proper permissions to avoid accidental exposure of services or data.

2. IP Whitelisting and Access Control:

- Since non-AWS IPs like `199.44.96.130` (for tlh.vrsystems.com) are present, it's important for VR Systems to ensure secure communication between AWS-hosted infrastructure and external or on-premises servers. IP whitelisting, VPNs, or secure tunnels like AWS Direct Connect should be used to safeguard these interactions.

3. DNS Security with DNSSEC:

- While DNS lookups are successful, the introduction of DNSSEC would provide an additional layer of protection by ensuring that DNS responses are not tampered with, especially for critical services like mta-sts.vrsystems.com or www.vrsystems.com.

4. Load Balancing and Availability:

- The use of multiple IP addresses for critical subdomains like texas.vrsystems.com and mta-sts.vrsystems.com ensures reliability. It's crucial to monitor the load balancing behavior across these IPs, ensuring that they are evenly distributing traffic and managing failover correctly.

Recommendations:

1. Regular Security Audits:

- Regular security audits should be performed on both AWS-hosted and externally hosted IPs to ensure that they comply with the latest security standards and follow best practices for encryption, access control, and threat monitoring.

2. Monitor IP Reputation:

P11

PAGE-028

- VR Systems should ensure that none of their IP addresses, especially those associated with email services (e.g., mta-sts.vrsystems.com) or content delivery (videos.cdn.vrsystems.com), are listed on any public IP blacklists. This will help maintain a strong email reputation and prevent service disruptions.

3. Integration of AWS Security Tools:

- AWS provides various tools to secure and monitor infrastructure, including GuardDuty for threat detection, CloudTrail for logging, and Security Hub for centralized security management. Integrating these tools will help VR Systems maintain visibility over their entire cloud infrastructure and detect any security anomalies.

Conclusion:

The IPv4 addresses associated with VR Systems point to a robust, cloud-based infrastructure primarily hosted on AWS, complemented by a mix of external hosting for certain subdomains. The infrastructure is well-distributed and makes use of redundancy and content delivery networks to ensure high availability and low latency. However, continuous monitoring, enhanced security practices, and ensuring integration between AWS-hosted and external services are essential to maintain the integrity and security of VR Systems' operations.

Analysis of Externally Referenced URLs

The externally referenced URLs found on the VR Systems website provide valuable insights into its dependencies, content sources, and third-party services. Here is an analysis of these URLs based on the data you provided:

1. Short.io Redirects and Cloudfront Links:

- URLs related to short.io (e.g., 'http://short.io/?utm_source=domain_blank_page' and 'http://short.io/?utm_source=link_not_found') indicate that some URLs or resources on VR Systems' pages may be using shortened links or custom domains managed by short.io for branding or redirect purposes.

- Several links point to CloudFront, AWS's content delivery network (CDN), such as:

- 'https://d2te5kruq0pvbl.cloudfront.net'
- These are likely used for optimizing the delivery of static assets (e.g., images) and ensuring better performance for users across the globe.

P17

PAUL - 029

2. CDN from ElectionsFL.org:

- Several assets, such as icons and images, are hosted on electionsfl.org, a domain associated with Florida's election systems (e.g., 'http://vrcdn.electionsfl.org/portals/vr/images/demo/wf_callusicon.png').
- This suggests that VR Systems is closely tied to Florida's election infrastructure and might be leveraging resources from this platform to enhance their web interface, such as using common iconography or branding elements.

3. Social Media and Tracking Pixels:

- External references include social media integration via Facebook and LinkedIn, indicating VR Systems' use of social platforms for marketing or user engagement.

- Example:

- '<https://www.facebook.com/vrsystemsinc>'
- '<https://www.linkedin.com/company/vr-systems-inc>'

- In addition, a Facebook tracking pixel (<https://www.facebook.com/tr?id=658956144580505&ev=PageView&noscript=1>) is in use, which suggests that the company is collecting user behavior data for marketing or performance analysis.

4. Third-Party Libraries and Fonts:

- VR Systems relies on several third-party libraries and font providers for their website's design and functionality. These include:
 - Bootstrap (<https://maxcdn.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css>) for responsive design and user interface components.
 - Typekit (<https://use.typekit.net/raw8oqu.js>) for custom fonts.
 - Fonts.net (<https://fast.fonts.net/jsapi>) for additional typography.
- These dependencies allow VR Systems to maintain a polished, responsive design across their website.

5. Third-Party Tools and APIs:

- Several URLs indicate reliance on third-party tools, such as:

117

PAGE 030

- Google reCAPTCHA (<https://www.google.com/recaptcha/api.js>), used to prevent bots and ensure secure form submissions.
- Google Maps (<https://goo.gl/maps/xM6Z32N47m4orGnJ6>), used to provide a map interface for their contact page.
- GitHub assets (<https://assets-cdn.github.com/images/icons/emoji/octocat.png>), suggesting they may have some open-source involvement or use GitHub for code or asset management.

6. Google and Microsoft Services:

- VR Systems uses URLs related to Google Services (e.g., <https://www.google.com/a/vrsystems.com/ServiceLogin>), which likely indicates internal or external email/calendar management via Google Workspace.
- Microsoft Edge and Google Chrome links (<https://www.microsoft.com/en-us/edge> and <https://www.google.com/chrome/>) suggest that the website provides browser compatibility information or recommendations to users, which could be part of a support or troubleshooting guide.

7. Partner and Client Links:

- Some URLs reference partner or client organizations:
 - MyFloridaElections (<https://www.myfloridaelections.com/Events/FSASE-Workshops-Conferences1>) and IAACR (<https://www.iaccr.net/Conferences.html>) suggest relationships with election systems and organizations in Florida and other regions.
 - These links imply collaborations with government agencies, associations, or events related to election management.

8. Calendar and Conference Resources:

- URLs such as ACCCIND (<https://acccind.org/>) and NCSBE (<https://projects.ncsu.edu/mckimmon/cpe/opd/NCSBE/>) indicate involvement in, or promotion of, conferences and workshops, particularly in the election or tech industries.
- Google Calendar Integration (<https://calendar.google.com/calendar/>) highlights possible use of Google Calendar for scheduling or event management, indicating that both public and internal calendar events are being managed.

9. Security and Compliance:

P11

PAGE - 031

- CI Security ('<https://www.cisecurity.org/press-release/the-center-for-internet-security-unveils-new-approach-to-verify-non-voting-election-system-security/>') suggests a focus on cybersecurity and compliance with standards for election security.

- This press release could be an important resource for VR Systems to ensure non-voting election systems are secure, underlining the company's commitment to protecting electoral processes.

Summary:

- Third-Party Integration: VR Systems uses a wide array of third-party services, from content delivery (CloudFront) to design (Bootstrap, Typekit), to ensure a responsive, secure, and visually appealing website.

- Election and Government Partnerships: The referenced URLs point to strong affiliations with Florida's election system and other election-related bodies, underscoring VR Systems' pivotal role in supporting election processes.

- Social Media and User Engagement: With links to Facebook, LinkedIn, and social tracking pixels, VR Systems actively engages with users through social platforms, which might be part of its public relations or marketing strategy.

- Security Compliance: The inclusion of resources like CI Security and Google reCAPTCHA indicates a strong focus on security, especially given VR Systems' critical role in election technologies.

Analysis of Linked URLs from VR Systems

The data you provided represents the results of a web spider scan that cataloged URLs from various subdomains of VR Systems. The spider primarily targeted several key domains and subdomains, collecting internal resources such as JavaScript files, CSS stylesheets, images, PDFs, and other web assets. Below is a detailed analysis of the findings:

1. Key Domains and Subdomains

- calendar.vrsystems.com: Appears to be a calendar system hosted on VR Systems, likely used for scheduling events or meetings related to the company's services.

PAI

PAIR - 032

- deploy.vrsystems.com: Deployment services or a system related to VR Systems' technology. This subdomain houses JavaScript files, CSS files, images, and other assets, including hashed assets.
- link.vrsystems.com: Contains references to link-related files, including favicon references and possibly placeholder URLs.
- mta-sts.vrsystems.com: A subdomain often related to Mail Transfer Agent Strict Transport Security (MTA-STS), which indicates the use of this for email security standards.
- tempest.vrsystems.com: No clear information based on URLs alone, but likely related to a project or service code-named "Tempest."
- texas.vrsystems.com: Potentially targeting users in the Texas region with specific services or content.
- tlh.vrsystems.com: Another subdomain potentially related to services focused on specific locations or business units.
- videos.cdn.vrsystems.com: Content distribution network (CDN) for hosting videos related to VR Systems.
- www.vrsystems.com: The main domain of VR Systems, with references to their primary services and web pages.

2. Types of Data Collected

- Web Pages: Core URLs linking to different sections of the main site, including "Request-a-Demo," "About Us," "Products," "Contact Us," and "Solutions." These represent the primary user-facing sections of the site.
- JavaScript and CSS Files: The spider discovered various JavaScript (e.g., 'jquery.js', 'dnn.js', 'vendor-react.js') and CSS files (e.g., 'bootstrap.min.css'). These files help render the website and provide functionality.
- Images: Several images were collected, including product images, icons, and company logos (e.g., 'flag.png', 'EVID-1.png'). These are used to visually represent the company's products and services.
- PDF Documents: Many PDFs were referenced (e.g., 'Press-Release-20191231.pdf', 'VR-Systems-Voter-Focus-Texas-Certification.pdf'), which seem to be either public relations materials or official documents related to certifications and services.
- Hashed Assets: The site appears to use a content delivery or asset hashing system, with many URLs referencing files like 'vendor.e04aac3f3610e7d76d1c[hashedasset.js]'. This indicates the use of hashed filenames for static resources, which is a common practice for optimizing browser caching and ensuring the latest versions of files are delivered to users.

P17 PAGE - 033

3. Noteworthy Findings

- Security and Vulnerabilities:

- The references to MTA-STS (mta-sts.vrsystems.com) imply that email security is in place, but the security of web-based resources (e.g., JavaScript, CSS, and HTML) should also be scrutinized.

- There are multiple references to JavaScript assets, including potentially older versions of libraries (e.g., 'jquery.js'), which could expose the system to vulnerabilities if not kept up to date.

- Public Documents and Resources:

- Many PDFs and public documents related to certifications, brochures, and press releases were discovered. Some of these documents (e.g., related to election certifications) could provide insights into the services offered by VR Systems in specific jurisdictions.

- These PDFs should be checked for potentially sensitive information that might have been inadvertently made accessible.

4. Organizational Insight

- The broad range of subdomains suggests that VR Systems has a multi-faceted digital infrastructure supporting various aspects of its business, from content distribution (videos, PDFs) to customer engagement (demos, product brochures) and region-specific services (Texas subdomain).

- The presence of distinct subdomains for deployments, email security, and resource hosting shows an organized approach to web operations. However, these subdomains also represent potential attack vectors if not properly secured.

5. Potential Security Implications

- Obsolete or Exposed Resources: The spider found several JavaScript, CSS, and image resources. If these resources are not maintained, vulnerabilities could arise, especially with older libraries (e.g., jQuery).

- Redundant or Placeholder URLs: Some URLs (like 'https://deploy.vrsystems.com/+/r+') appear to contain placeholders or development remnants. These should be investigated, as they might indicate unintentional exposure of debugging or development code.

- Publicly Accessible Documents: While many PDFs appear to be intended for public consumption, it is essential to review these for sensitive content (e.g., internal reports, election data) to prevent data leaks.

P17

PAGE - 034

6. Recommendations for Next Steps

- Security Review: Conduct a thorough security audit of the JavaScript libraries and CSS files found by the spider. Outdated or vulnerable versions of popular libraries could expose the site to security risks.
- URL Cleanup: Review the placeholder or potentially malformed URLs (e.g., 'https://deploy.vrsystems.com/+/a+') to ensure no development or debugging URLs are exposed to the public.
- Document Audit: Although most of the PDFs found seem innocuous, they should be reviewed for sensitive information, especially if they pertain to certifications, internal processes, or customer contracts.
- Image Optimization: Many images were found during the scan. Consider optimizing these for performance (e.g., reducing file size, serving them through a CDN) to improve site loading times.

Summary

The scan provides valuable insights into the structure and resources of the VR Systems website, uncovering various web pages, documents, scripts, and images. While many of these assets appear standard, attention should be given to the security of JavaScript libraries and potential exposure of sensitive documents.

Analysis of Information from Malicious Links

This analysis focuses on two findings from the scan of potentially malicious links or IP addresses, both linked to the IP range '54.208.0.0/15'. This range is connected to reports from PhishStats, CleanTalk, and VoIPBL. Below is an in-depth analysis of the significance and potential risks associated with these findings:

1. PhishStats Finding

- Updated: 2024-09-07 19:12:14
- Module: 'sfp_phishstats'
- Source: '54.208.31.55'
- Data: PhishStats [54.208.31.55]

P17

PAGE 035

Analysis:

- PhishStats is a platform that tracks phishing activities globally by logging malicious domains and IP addresses used in phishing schemes.
- 54.208.31.55: The specific IP address from this range has been flagged by PhishStats, indicating its association with phishing activities.

- Risks:

- Phishing attacks are one of the most common methods for stealing sensitive information, including login credentials, financial data, or access to systems.
- If this IP or associated systems are interacting with your infrastructure (e.g., through emails, links, or forms), there is a high risk of phishing attempts targeting your users.
- If users mistakenly interact with resources originating from this IP, it could result in compromised credentials, ransomware, or malware deployment.

- Recommendations:

- Block or closely monitor any traffic originating from or attempting to communicate with '54.208.31.55'.
- Educate users on identifying phishing schemes and direct them to report any suspicious emails, links, or activities associated with this IP.
- Implement email filtering solutions to ensure phishing emails originating from this or similar IPs are blocked.

2. CleanTalk and VoIPBL Blacklists

- Updated: 2024-09-07 19:26:08
- Module: 'sfp_cleantalk', 'sfp_voipbl'
- Source: '54.208.0.0/15'
- Data:
 - CleanTalk Spam List [54.208.0.0/15]
- Reference:
 - [https://iplists.firehol.org/files/cleantalk_7d.ipset]

PAGE - 036

- VoIP Blacklist (VoIPBL) [54.208.0.0/15]

- Reference:

<https://voipbl.org/check/?ip=54.208.0.0/15>

Analysis:

- CleanTalk and VoIPBL are both well-established blacklist services:

- CleanTalk: Specializes in detecting and blocking spam across web platforms, focusing on IP addresses known for generating unwanted or malicious traffic.

- VoIPBL: A real-time blacklist specifically designed to prevent VoIP fraud and abusive activities linked to telephony systems. It identifies VoIP-related abuse, including toll fraud, robocalls, and other unwanted behaviors.

- 54.208.0.0/15: This IP range, which includes the aforementioned flagged IP ('54.208.31.55'), is broad and potentially encompasses numerous servers. Being listed in both CleanTalk and VoIPBL suggests:

- Spam and Fraudulent Activities: This IP range has likely been associated with sending spam, fraudulent telephony activities, or unauthorized access attempts.

- VoIP-specific Threats: For organizations using VoIP systems, the inclusion in VoIPBL indicates that there is a significant risk of fraud, call spoofing, or toll fraud attacks originating from this IP range.

- Risks:

- Organizations interacting with this range for VoIP services may face fraudulent attempts, toll fraud, or be exposed to compromised communication channels.

- Spam originating from this range could cause issues such as network slowdowns, unsolicited traffic, or phishing attempts.

- Recommendations:

- Block or restrict access to the entire IP range ('54.208.0.0/15') within your network's firewall or security configurations.

- If VoIP services are in use, ensure that your systems are updated and that security measures like rate limiting, call authentication, and fraud detection systems are in place to mitigate VoIP fraud.

- Implement anti-spam solutions (e.g., spam filters, Captchas) to protect users from potential spam originating from this range.

- Review VoIP traffic and logs for any suspicious activity that may be tied to this IP range.

P17

PAGE - 037

Summary of Risks and Actions

1. Phishing Risks (54.208.31.55):

- Flagged by PhishStats for involvement in phishing activities.
- Potential for phishing emails, malicious links, or credential theft originating from this IP.

Action: Block the IP and monitor closely for any phishing-related activity.

2. Spam and VoIP Threats (54.208.0.0/15):

- Identified by CleanTalk for spam activities and by VoIPBL for VoIP-related fraud.
- Risks include telephony fraud, call spoofing, spam messages, and potentially unwanted traffic.

Action: Block or monitor traffic from the entire IP range. Ensure VoIP systems have proper security measures.

Analysis of Netblocks (IPv6 and IPv4)

This analysis covers the netblocks found in two tabs, one dealing with IPv6 ('2600:9000:20d1::/48') and the other dealing with IPv4 netblocks such as '207.174.61.0/24', '34.192.0.0/12', and '54.156.0.0/14'. Here's a detailed breakdown:

1. IPv6 Netblock: '2600:9000:20d1::/48'

- Updated: Multiple timestamps between 2024-09-07 19:02 and 2024-09-07 19:30.
- Sources: 'sfp_ripe', 'sfp_bgpview'.
- IP Prefix: '2600:9000:20d1::/48'.

PN PAUL - 0308

Analysis:

- This IPv6 range is relatively large ('/48'), indicating that it can host up to 65,536 subnets, each with a significant number of IPv6 addresses.
- The repeated findings from 'RIPE' and 'BGPView' modules suggest that this netblock has been publicly announced and is visible across internet routing tables.
- Given that this netblock appears multiple times, it is possible that this IPv6 range is actively being utilized in a broad deployment, possibly for cloud-based infrastructure or large-scale web services.

Potential Usage:

- Cloud Providers: It is likely that this range is part of the IP space assigned to a large-scale cloud provider (e.g., Amazon AWS, Google Cloud, or similar) based on the size and usage pattern.
- CDN or Hosting: IPv6 blocks of this scale are often associated with content delivery networks (CDNs) or web hosting providers due to the need for large IP allocations.

Risks:

- There is no immediate indication of malicious activities from this netblock. However, the large size and presence in global routing suggest it could be a target for misuse, especially if it's part of a public cloud.
- If this netblock is associated with a CDN or hosting provider, there may be diverse entities using it, some of which could be involved in unwanted activities (e.g., spam, DDoS attacks).

Recommendations:

- Monitoring: If your infrastructure interacts with this IPv6 range, continuous monitoring for unusual activities is recommended.
- Access Control: Consider restricting access to critical infrastructure from this netblock unless necessary.
- Contextual Understanding: Investigate further if this range is linked to a specific service or provider you are dealing with, especially for cloud services.

P19

PAGE - 039

2. IPv4 Netblocks

Netblock 1: `207.174.61.0/24`

- Updated: 2024-09-07 19:35.
- Sources: `sfp_ripe`, `sfp_bgpview`.
- Description: This is a small `/24` range (256 IP addresses), typically assigned to a specific organization.

Analysis:

- The `207.174.61.0/24` netblock appears to be allocated for a small or medium-sized enterprise or dedicated infrastructure (e.g., datacenters, ISPs, or corporate networks).
- Given its smaller size, this netblock is less likely to be associated with large-scale cloud providers but could still be used for web hosting, business services, or smaller ISP allocations.

Risks:

- Target for Malicious Activity: Smaller netblocks are often scrutinized less than large cloud ranges, making them potential targets for hosting malicious content, especially if the owner of the IP range is not vigilant.
- Limited Attribution: Without further details on the organization using this range, it is difficult to attribute specific risk. This range should be monitored if traffic is seen originating from or targeting this block.

Recommendations:

- Block/Allowlist Consideration: Depending on the specific services originating from this block, it may be necessary to block or allowlist it.
- Further Investigation: Investigate whether this netblock belongs to a known service provider or entity that could impact your organization.

Netblock 2: `34.192.0.0/12`

- Updated: 2024-09-07 19:32.

PAGE - 040

- Sources: `sfp_ripe`, `sfp_bgpview`.
- Description: A large `/12` block, providing over 1 million IP addresses.

Analysis:

- The size of this netblock suggests it belongs to a large organization, most likely a cloud provider (Amazon AWS, Google, or similar).
- Commonly used for cloud-hosted services: AWS is a common candidate for this range (`34.x.x.x`), and it's likely used for various applications, websites, or backend infrastructure.

Risks:

- High Potential for Mixed Usage: Given the size and likely cloud usage, this netblock will host numerous services, ranging from legitimate businesses to potential malicious actors leveraging cloud resources.
- Hard to Block Entirely: Blocking such a large range outright is impractical due to its association with numerous legitimate services.

Recommendations:

- Selective Monitoring: Monitor specific traffic originating from IPs within this block rather than blocking the entire range.
- Usage-based Restrictions: Only block or allow specific IP addresses if there is evidence of suspicious activity related to your organization.

Netblock 3: `54.156.0.0/14`

- Updated: 2024-09-07 19:33.
- Sources: `sfp_ripe`, `sfp_bgpview`.
- Description: A `/14` range, offering over 250,000 IP addresses.

Analysis:

PA

Page 041

- This range is commonly associated with Amazon Web Services (AWS), a dominant player in the cloud infrastructure space.
- Large `/14` ranges such as this are frequently used for hosting a wide variety of services, including websites, APIs, databases, and more.

Risks:

- Similar to the previous large netblock, AWS-hosted ranges are a mixed bag of legitimate and potential malicious actors.
- Potential for Abuse: Cybercriminals can leverage cloud platforms like AWS to quickly scale malicious activities (e.g., phishing, DDoS attacks) before cloud providers can mitigate them.

Recommendations:

- Traffic Analysis: Be cautious with inbound and outbound traffic to IPs within this range. Traffic should be evaluated on a case-by-case basis.
- Cloud Provider Engagement: AWS is generally responsive to abuse reports, so suspicious activities linked to this range should be reported directly to AWS.

Netblock 4: `54.208.0.0/15`

- Updated: 2024-09-07 18:52.
- Sources: `sfp_ripe`, `sfp_bgpview`.
- Description: Another large AWS netblock (`/15`), covering over 130,000 IP addresses.

Analysis:

- As with the previous AWS-associated ranges, this block is likely used for various services hosted on AWS, including websites, APIs, and backend systems.
- Similar risk assessments apply as AWS provides flexible hosting options that could be used by both legitimate and malicious entities.

Risks and Recommendations:

- Mixed-Use Risks: This block is likely hosting both legitimate services and potential bad actors.

PAGE - 042

P17

- Recommendation: Focus on identifying specific bad actors within this range using more granular IP intelligence tools.

Conclusion

- IPv6 Netblock `2600:9000:20d1::/48`: Large-scale allocation likely associated with cloud providers or CDNs, requiring continuous monitoring.
- IPv4 Netblocks:
 - Ranges like `34.192.0.0/12` and `54.156.0.0/14` are commonly AWS-associated and present mixed risks due to cloud-based hosting.
 - Smaller netblocks like `207.174.61.0/24` may be tied to smaller organizations or ISPs and require specific monitoring.

Analysis of Three Tabs Regarding Providers Involved

1. Tab 1 - DNS Information:

- Provider: Amazon Web Services (AWS) and GoDaddy.
- Updated Entries:
 - Domains related to VR Systems (e.g., `vrsystems.com`) are pointing to various AWS DNS servers.
 - Domain control information is linked to GoDaddy nameservers (`ns51.domaincontrol.com` and `ns52.domaincontrol.com`), which suggests that GoDaddy is the registrar and DNS hosting provider for the main domain (`vrsystems.com`), while the subdomains and services (like `mstats`, `videos.cdn`) are hosted via AWS DNS.

Analysis:

- AWS Involvement: Amazon Web Services is handling the DNS for VR Systems' subdomains, indicating that these specific services (likely related to email and video/CDN content) are hosted or routed through AWS infrastructure.
- GoDaddy: The main domain (`vrsystems.com`) is registered and managed via GoDaddy, which is a common registrar and DNS provider. However, more granular services have been offloaded to AWS for scalability and global distribution.

~~PII~~

PAGE - 043

Risks:

- AWS, being a large cloud provider, is often a target for abuse, and therefore, services hosted there may be at risk if not properly configured and monitored.
- There's no immediate sign of misconfiguration, but it's essential to continuously monitor DNS changes and AWS-hosted services for potential vulnerabilities.

Recommendations:

- Ensure DNSSEC: If not already enabled, DNSSEC should be implemented to safeguard against spoofing attacks.
- AWS Monitoring: Utilize AWS CloudTrail and DNS monitoring tools to track any malicious changes or abnormal activity.

2. Tab 2 - Hosting Providers (AWS & Microsoft Azure):

- Provider: Amazon Web Services (AWS) and Microsoft Azure.
- Updated Entries:
 - IP addresses such as '54.208.31.62', '52.22.23.138', and others are hosted on AWS infrastructure.
 - Additionally, '52.177.184.148' is associated with Microsoft Azure, meaning some of the services VR Systems uses are diversified across major cloud platforms (AWS and Azure).

Analysis:

- AWS Dominance: Most of the hosting appears to be within AWS, which is typical for many modern web services that require scalable, reliable cloud infrastructure.
- Azure Involvement: A single instance involving Microsoft Azure suggests that VR Systems may be leveraging different platforms for redundancy, performance, or region-specific requirements.

Risks:

P17

PAGE - 644

- While using both AWS and Azure provides scalability and fault tolerance, these platforms can also be attractive for cyberattacks, especially if the services are not adequately hardened.
- The risk of cloud provider abuse (e.g., compromised accounts or services being misused) should be continuously mitigated by following best practices in cloud security, including strong authentication and monitoring.

Recommendations:

- Cloud Security: Utilize the security services offered by both AWS and Azure, such as AWS Shield, AWS WAF, and Azure Security Center to harden the infrastructure.
- Multicloud Strategy: Continue leveraging multiple cloud providers to prevent single points of failure, but ensure consistent security policies are in place across all platforms.

3. Tab 3 - Page Info (HTML/Meta Data):

- Provider: VR Systems' official website.
- Updated Entries:
 - The meta tags and content provided in this tab belong to various sections of the VR Systems website (e.g., careers, products, privacy policy).
 - Several links are found for loading external JavaScript from Typekit (<https://use.typekit.net/raw8oqu.js>) and Google Recaptcha (<https://www.google.com/recaptcha/api.js>).

Analysis:

- External Dependencies: The website uses external resources from Adobe Typekit and Google (Recaptcha), which are commonly used for font rendering and bot protection respectively. This is a normal practice but does introduce reliance on third-party services.
- Potential Risks: Any external resource dependencies (like Typekit or Google APIs) increase the risk vector. If those third-party services were compromised, they could introduce security risks to the site (e.g., serving malicious scripts).
- Robust Meta Tag Usage: The website appears to be well-structured, with correct usage of meta tags (e.g., 'robots', 'content-type'), which is beneficial for SEO and security (e.g., proper indexation policies).

PLM

PAGE 045

Risks:

- Third-Party Service Risks: The reliance on external providers (e.g., Typekit and Google) means the site is dependent on their availability and security.
- Recaptcha Misuse: Google Recaptcha is widely used to prevent spam and bot submissions. However, improper configuration of security features may lead to vulnerabilities.

Recommendations:

- External Script Monitoring: Continuously monitor external resources to ensure they are serving valid content. Consider implementing Subresource Integrity (SRI) hashes to verify the integrity of scripts.
- Security Headers: Ensure that security headers like 'Content-Security-Policy' (CSP) are enforced to prevent XSS (Cross-Site Scripting) attacks, especially due to external script loading.

General Conclusion:

- VR Systems is utilizing both AWS and Azure cloud platforms for hosting and DNS services, ensuring robust and scalable infrastructure. The combination of these platforms provides flexibility but also introduces the need for strict monitoring and security controls to mitigate potential abuse.
- Third-party dependencies on services like Adobe Typekit and Google Recaptcha introduce risks related to external script handling, which should be monitored to prevent security breaches.
- The company's web presence is built with standard modern practices, but improvements in security monitoring (for both DNS and external scripts) are recommended to further strengthen its security posture.

Here's a breakdown of the raw data from DNS, file metadata, and RIR data sections:

Raw DNS Data Analysis:

- `calendar.vrsystems.com`: This domain resolves to a CNAME record that points to '`ghs.google.com`', which suggests that it uses Google-hosted services, possibly Google Sites or Google Apps.

9/29 046

- videos.cdn.vrsystems.com: This domain is associated with CloudFront (Amazon's CDN). It uses various AWS DNS services for redundancy ('ns-927.awsdns-51.net', etc.), indicating that media content is distributed via AWS CloudFront, a global content delivery network.
- mta-sts.vrsystems.com: This domain uses a CNAME that resolves to another CloudFront endpoint ('d36xwd7stvtot8.cloudfront.net'). This is part of an MTA-STS setup, used to enforce TLS for email communications, indicating email security measures.
- link.vrsystems.com: The CNAME points to 'cname.short.io', a URL shortening service. This suggests that 'link.vrsystems.com' is used to generate short URLs via Short.io.
- texas.vrsystems.com: This domain resolves to an AWS Elastic Load Balancer ('elb.amazonaws.com'), indicating that the Texas subdomain of VR Systems is likely load-balanced across multiple servers, providing high availability.

Raw File Metadata Analysis:

- The binary data under the 'sfp_binstring' module appears to represent hex values that correspond to images hosted on VR Systems' website ('<https://www.vrsystems.com>'). These are likely related to image icons on their platform, such as solution and product icons. The structure suggests either an encoded or low-level format representation of image metadata.

Raw RIR (Regional Internet Registry) Data Analysis:

- Jonathan Harris and VR Systems: Information about Jonathan Harris is tied to VR Systems, located in Tallahassee, Florida, and registered with ARIN. This confirms the identity of the person responsible for managing these network resources.
- 54.208.31.55 (Ashburn, VA): The IP is associated with Amazon Web Services (AWS) in Ashburn, Virginia, part of the AWS infrastructure. This reaffirms that VR Systems uses AWS as its hosting provider.
- 54.208.31.62 and other Amazon-related IPs: Similar to above, these IPs are part of Amazon's cloud infrastructure used by VR Systems, further highlighting their reliance on AWS services for hosting.

This data collectively demonstrates that VR Systems uses Amazon Web Services extensively for hosting, content delivery, email security, and various other services. Their reliance on AWS's global infrastructure likely provides scalability, reliability, and security for their systems.

The detailed analysis of the open ports on the website can be broken down by identifying common services associated with each port and analyzing potential security implications:

PA
PAGE - 047

1. Common Services Detected:

- Port 80 & 443: HTTP and HTTPS services. These are standard for web traffic. Port 443 is secured with SSL/TLS encryption, while port 80 is unencrypted. The presence of both ports indicates standard web server services.
- Port 22: SSH, used for secure shell access to the server. This port is often a target for brute-force attacks, so it should be secured with strong credentials and multi-factor authentication.
- Port 21: FTP, used for file transfers. If this service is exposed, it can be vulnerable to interception unless encrypted (e.g., FTPS).
- Port 3306: MySQL database. This port is commonly exposed on databases and could be vulnerable to unauthorized access. Best practice is to restrict access to trusted IPs.
- Port 3389: Remote Desktop Protocol (RDP). If exposed to the internet, RDP is a common target for brute-force attacks, leading to potential unauthorized server access.
- Port 53: DNS service, used for resolving domain names. DNS services can be vulnerable to DNS amplification attacks if not properly configured.
- Ports 110, 143, 993, 995: These are associated with email services (POP3, IMAP, and their secure versions). If exposed, these services could be a target for interception or data theft.
- Port 445: SMB/CIFS used for file sharing. This port has been associated with vulnerabilities like the WannaCry ransomware attack and should be protected.
- Port 137-139, 445: These are NetBIOS services for file sharing in Windows environments and can be a vector for exploitation in poorly secured environments.
- Port 123: NTP (Network Time Protocol). While less critical, NTP can be leveraged for DDoS amplification attacks if exposed.
- Ports 5900-5903: VNC, used for remote desktop access. Exposed VNC ports can be exploited for unauthorized remote access.

2. Risk Analysis:

- High-Risk Ports: Ports like 22 (SSH), 3389 (RDP), and 445 (SMB) are frequently targeted by attackers for unauthorized access, particularly if weak credentials are used or if the services are not configured securely.
- Database Ports: Exposure of MySQL (3306) and other database-related ports such as PostgreSQL (5432) poses a significant risk, especially if they are not protected by firewalls or access controls.

P(1) PAGE - 048

- File Sharing & Email Ports: Ports related to file sharing (SMB, FTP) and email services (POP3, IMAP) can be exploited for data breaches or man-in-the-middle attacks if not properly secured (e.g., using encryption or VPNs).

3. Best Practices:

- Restrict Port Access: Limit access to sensitive ports (e.g., 3306 for MySQL, 3389 for RDP) to known, trusted IP addresses. Use VPNs or firewalls to control who can access these services.
- Use Strong Authentication: Implement multi-factor authentication (MFA) for SSH and RDP services to mitigate the risk of brute-force attacks.
- Encrypt Traffic: For services like FTP (Port 21) or email protocols (POP3, IMAP), ensure encryption is enforced (e.g., FTPS, SMTPS, etc.).
- Close Unused Ports: Any ports not actively used should be closed to minimize attack surfaces.
- Patch Management: Regularly update all services running on these ports to mitigate vulnerabilities associated with outdated software.

The variety of open ports indicates that multiple services (e.g., web servers, remote access, file sharing, email) are running. This configuration can create multiple points of vulnerability, particularly if the system isn't adequately secured. Therefore, auditing, limiting exposure, and enhancing security configurations across these services are crucial steps for minimizing potential threats.

F18-

PAGE-001

FOR IMMEDIATE RELEASE

August 21, 2024

STATEMENT FROM VR SYSTEMS, INC.

Clarification on Florida Supervisors Of Elections County Website Issues

From Ben Martin, VR Systems Chief Operating Officer

"We want to clarify our response to what happened yesterday to the websites we host for county supervisors of elections in Florida.

"All of the customers websites that we host were impacted and we take full responsibility.

"The websites were down as we took steps to correct issues that were caused by logging that was enabled as a security measure on the sites. Once we resolved this, all of the sites were restored.

"To ensure this doesn't happen again, we have begun working with external technical experts to assist us with further analyzing and optimizing our system."

119 PAGE - 001



Outlook

Your Palm Beach County - SOE public records request #24-1075 has been opened.

From Palm Beach County - SOE Public Records <messages@nextrequest.com>

Date Tue 10/1/2024 7:39 AM

To Jeff Buongiorno <jeff@etektraining.com>

-- Attach a non-image file and/or reply ABOVE THIS LINE with a message, and it will be sent to staff on this request. --

Palm Beach County - SOE Public Records

Your record request #24-1075 has been submitted successfully.

Your public records request has been received and is currently being reviewed. The reference number to your request is provided below.

If you need to edit your request, you may "open form" and update as needed.

Respectfully,

Public Records

The due date for your request may be later than usual because the office is closed on:

- October 3: Rosh Hashana
- October 14: Indigenous Peoples Day (Columbus Day)

P10

PAGE - 002



Mail Ballot Request Confirmation

From noreply@vrsystems.com <noreply@vrsystems.com>

Date Mon 2/26/2024 7:41 AM

To Jeff Buongiorno <jeff@etektraining.com>

Jeffrey Buongiorno,

A vote-by-mail request for the 2024 Pres Preference Primary election on 03/19/2024 was submitted to the elections office for you on 02/26/2024 at 07:41 AM.

Your mail ballot for this election will be sent to the following address:

3851 N Ocean Blvd 406
Gulf Stream FL 33483

If this request was made on your behalf by someone else, their information is as follows:

Requested By:

Requester's Specified Relationship to You:

Requester's Address:

If you have any questions or need further assistance, please contact your local elections office for assistance.

123291683



P2Q - PAGE - 001

August 12, 2024

Bernard Jessen
3286 Arcara Way
Apt. 302
Lake Worth, FL 33467

VIA U.S. MAIL AND CERTIFIED MAIL
RETURN RECEIPT REQUESTED

Re: Protested Voter Signatures

Dear Mr. Jessen,

On July 30, August 2, and August 6, 2004 you filed official protests against acceptance of ballots from a total of forty-one (41) voters in Palm Beach County, Florida based upon your review of the signature of the voters in their official voter registration file and the signatures appearing on their returned vote-by-mail ballots that you observed during your inspection thereof as a candidate, a political party official, or a political committee official, or an authorized designee thereof in accordance with sec. 101.572, F.S. Please be advised that the Canvassing Board accepted all protested ballots due to the signatures on the returned envelopes being nearly identical matches to the voters' signatures contained in their voter records.

As a candidate, a political party official, or a political committee official, or an authorized designee thereof, you should be aware that section 101.111, F.S. makes it a crime to frivolously challenge a person's right to vote.¹ Because the signatures on the vote-by-mail ballot envelopes of all 41 voters were nearly exact matches, the Palm Beach County Canvassing Board considers each of the 41 protests to be frivolously filed and has notified law enforcement, the statewide elections crimes office and the State Attorney's office for further investigation and possible prosecution.

Respectfully,


Stacey J. Manning, Esq.
Canvassing Board Attorney

¹ "Any elector or poll watcher filing a frivolous challenge of any person's right to vote commits a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083; however, electors or poll watchers shall not be subject to liability for any action taken in good faith and in furtherance of any activity or duty permitted of such electors or poll watchers by law. Each instance where any elector or poll watcher files a frivolous challenge of any person's right to vote constitutes a separate offense." See sec. 101.111(2), F.S.